DataSMART® 656 and 658 T1 DSUs User's Guide

72656DataSMART 656, DSU with Ethernet

72658DataSMART 658, Add/Drop DSU with Ethernet

Document #5000145

KENTROX®
A Platinum Equity Company

Copyright

Specifications published here are current or planned as of the date of publication of this document. Because we are continuously improving and adding features to our products, Kentrox reserves the right to change specifications without prior notice. You may verify product specifications by contacting our office.

In no event shall Kentrox be liable for any damages resulting from loss of data, loss of use, or loss of profits. Kentrox further disclaims any and all liability for indirect, incidental, special, consequential or other similar damages. This disclaimer of liability applies to all products, publications and services during and after the warranty period.

Trademark information

Kentrox and DataSMART are registered trademarks of Kentrox, LLC. DataSMART MAX, DataSMART SPort, and M-PATH are trademarks of Kentrox, LLC.

All other product names are trademarks or registered trademarks of their respective owners.

Revision history

Part #	Date	Description
65-72658101	June, 1997	Issue 1
5000145	December, 2001	Issue 2

Contents

Chapter 7 Troubleshooting

Chapter 8 Using network management

Preface

This manual contains a detailed description of all operations of the DataSMART 656 and 658 Data Service Units (DSUs). It provides specific information for configuring the DataSMART units and for using them to monitor and troubleshoot your T1 circuit's performance. It also provides detailed listings of all DataSMART menus, commands, and specifications.

Who should read this manual?

This manual is intended as a reference source for ongoing operation of the DataSMART 656 and 658 DSUs. It covers all possible operations and configuration choices in detail. For initial installation, power up, and basic configuration of the units, we recommend that you first turn to the *DataSMART 600 Series Installation Guide*. Note that installation and service should be performed only by trained and qualified personnel.

Viewing this manual as a PDF file

This manual is designed to be used as both a printed book and a PDF file, and includes the following features for PDF viewing:

- Cross-references are clickable hyperlinks that appear in blue text.
- Chapters and section headings are represented as clickable bookmarks in the left-hand pane of the Acrobat viewer.
- Page numbering is consistent between the printed page and the PDF file to help you easily select a range of pages for printing.

You can obtain PDF files of our manuals by visiting http://www.kentrox.com.

Related documentation

In addition to this manual, the following are available:

- *DataSMART 600 Series Installation Guide*
- *Kentrox DSU/CSU MIB Reference*, available in our World Wide Web on-line library at http://www.kentrox.com.

MIB source files

MIB source files are available by visiting http://www.kentrox.com/support.

About this manual

This manual contains the following information:

"Preface" (this section) explains the purpose and organization of this manual, and tells how to contact Kentrox Customer Support if you run into difficulties.

"Introduction" describes the applications and features of the DataSMART.

"Entering commands and logging in" introduces you to the DataSMART command-line and front-panel interfaces and explains how to log in.

"Establishing system security" shows how to secure the unit's command-line and front-panel interfaces.

"Configuring the system" describes in detail all of the system-level configuration choices you can make. This includes specifying the system source clock, configuring the alarm message output, and configuring the DCE and DTE control ports.

"Configuring interfaces" describes in detail all the configuration choices available for the network interface, the terminal interface, and the data ports, as well as assigning channels.

"Performance monitoring" shows you how to access and use the DataSMART T1 performance reports, alarm history report, and security history report.

"Troubleshooting" shows you how to use the DataSMART to recognize and troubleshoot abnormal conditions in your T1 circuit. It describes the front-panel LEDs, alarm messages, system status displays, and diagnostic tools such as loopbacks and BERTs.

"Using network management" shows you how to set up and use the DataSMART in an SNMP network management environment and how to manage its Ethernet, T1 data link, or serial-port IP interfaces. It also describes the embedded SNMP agent and Telnet link.

"Quick reference" summarizes DataSMART menus and commands and also provides a comprehensive listing of product specifications.

At the back of the manual, you'll also find a glossary of terms and an index.

Conventions used in this manual

This manual employs the following conventions when explaining command-line syntax:

Literals	Bold type identifies commands and syntax elements that must be entered exactly as shown in the text.
Variables	Italic type identifies variable syntax elements, such as values or alphanumeric strings you can enter.
x|*y*	A vertical line between elements means that the elements are mutually exclusive; you can select one and only one of the elements.
[ ]	Brackets indicate items that are optional.

Who to call for assistance

If you need assistance with this product or have questions not answered by this manual, please visit our Support page on the Kentrox Web site. You are also welcome to call or send email to our Technical Assistance Center. Please have your product's software revision and hardware serial numbers available to give to the Support representative. All product returns must include a Return Authorization number, which you can obtain by calling the Technical Assistance Center.

The numbers listed below are current at the time of publication. See the Kentrox Web site for detailed contact and warranty information.

1-800-733-5511 (continental USA only)
1-503-350-6001
email: support@kentrox.com
http://www.kentrox.com

C H A P T E R

1 *Introduction*

The DataSMART Model 656 and 658 data service units (DSUs) provide in-band managed digital service access to T1 and fractional T1 lines. DataSMART units connect PBXs, switches, routers, and other customer premise equipment to the T1 service. You can use SNMP to manage the units remotely via one or more of these methods: data link on the T1 line (using a facility data link, 8 Kbps borrowed from a DS0 channel, or a full DS0 channel), via Ethernet, or using the SLIP or PPP protocols on a control port.

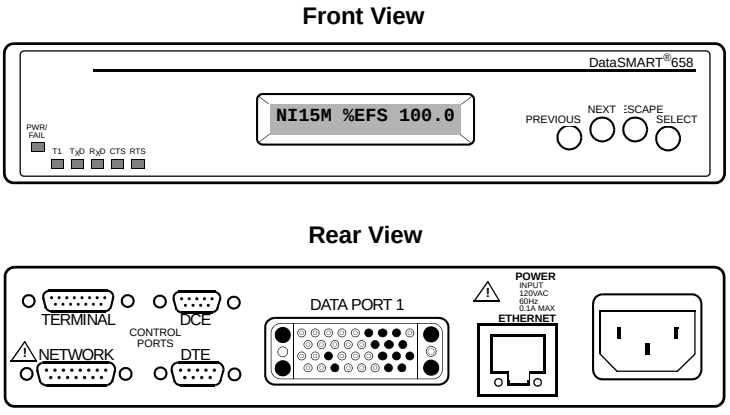
When the optional Frame Relay board is installed, these DataSMART units are converted to DataSMART 656-F and 658-F Frame Relay Monitoring DSUs. Functionally identical to the DataSMART Model 686 and 688, they also monitor frame-level performance of your T1/FT1 frame service (Frame Relay, ATM FUNI or ATM DXI).

This user's guide covers two basic DataSMART configurations:

- The Model 656 DSU, with one data port and an Ethernet management port
- The Model 658 add/drop DSU, with one data port, an Ethernet management port, and a terminal interface

All models are housed in the same one-unit-high (1U) rack-mount box.

Figure 1—The DataSMART 658



These figures show a single-port add/drop DSU/CSU with an Ethernet management interface. The DataSMART unit you are working with may not contain some of the ports shown here.

Features of the DataSMART

A front-panel interface for easy installation

- LCD-and-push button interface can be used to completely configure a DataSMART
- Intuitive interface simplifies troubleshooting

IP-based network management (all units)

- You can configure, monitor, and troubleshoot individual units using standard network management tools
- IP interface generates traps when network events occur
- Unit responds to pings
- IP interface allows Telnet access
- Unit supports MIB II (for LAN-based hosts), the DS1 MIB (for T1 line management), and an Enterprise MIB (which allows SNMP access to all commands available via the control port menu interface; this includes performance monitoring, diagnostics and reconfiguration).

Options for IP management connectivity

- IP interface allows data-link access to remote stand-alone units over Facility Data Link (FDL) or DS0 channel: FDL requires Extended Super Frame (ESF) framing on the T1 line; DS0 can be idle or assigned to the data port
- Data-link IP management data rate can be 56 or 64 Kbps (idle DS0); 8 Kbps (DS0 assigned to data port); or 4 Kbps (FDL)
- Ethernet access is available via a 10Base-T connector
- Serial-port access is available via the asynchronous serial connection using SLIP or PPP protocol
- Units can be daisy-chained via control ports using SLIP protocol

T1 performance monitoring

- Reports show details of T1 interface performance
- Unit retains T1 summary report data for seven days while powered up
- Unit provides separate T1 network interface reports for user and carrier
- Unit provides detailed terminal interface reports (Model 658)

T1 diagnostics

- LEDs and front panel display indicate problems at the network interface, data ports, and Ethernet interface
- LEDs and front panel display indicate problems at the terminal interface (Model 658)
- Unit allows T1 access loopbacks to be set remotely or locally
- Unit contains a built-in test code generator and bit error rate test (BERT) to test the T1 access line
- User interface shows real-time status of system

Security features

- IP source address screening rejects IP packets from unauthorized hosts
- Telnet password provides security for remote logins
- Authentication traps report failed Telnet login attempts, SNMP community strings, and IP packets received from invalid IP hosts
- Control port access protected by three levels of user password
- LCD access password protects unit from unauthorized access to front panel
- LCD operates in read-only or read/write mode

Nonvolatile memory

- Retains unit's configuration for five years minimum without power.

Compatibility

- ARC remote login capabilities are fully compatible with all DataSMART 500 and 600 series DSU/CSUs, DataSMART MAX/SPort DSU/CSUs, and M-PATH CSUs
- In-band data link management is fully compatible with DataSMART 554/558 DSU/CSUs and all M-PATH CSUs

CHAPTER

2 *Entering commands and logging in*

This chapter describes:

- Entering commands via the command-line interface
- Entering commands via the front-panel interface
- Logging into the DataSMART

Using the DataSMART

With the command-line interface you use a terminal to manage and monitor the DataSMART DSU.

Using the command-line interface

The DataSMART command-line interface is accessible through various physical connections:

- Telnet via the Ethernet 10BaseT connector
- Telnet or ARC link to a remote unit over a facility data link within the T1 data stream (available with ESF framing only)
- Telnet over the facility data link or DS0 data link within the T1 data stream
- Telnet via a PPP/SLIP connection to the unit's DCE or DTE control port
- ASCII (non-IP) connection to the control port

Menus vary according to your DataSMART model. Some commands apply only to the DataSMART 658 add/drop unit with the Ethernet connector.

Figure 2—The Main menu

```
DataSMART 6nn Version 1.nn Copyright (c) 1997 Kentrox
        ADDRESS: 00:00:000      NAME: PORTLAND,OR

MM                      - Main Menu
SS                      - System Status and Remote Menu
R                       - Reports Menu

LM                      - Local Maintenance Menu
RM                      - Remote Maintenance Menu

AC                      - Alarm Configuration Menu
CC                      - Control Port Configuration Menu
DC                      - Data Port Configuration Menu
FC                      - Fractional T1 Configuration Menu
MC                      - Management Configuration Menu
NC                      - NI Configuration Menu
PC                      - Password Entry and Configuration Menu
SC                      - System Configuration Menu
TC                      - TI Configuration Menu

^D                      - Logout
^D<xx>:<yy>:<zzz>^E     - Address Another Unit

MM>
```

DataSMART 658 only — TC

To see one of the menus, enter the menu name at the prompt. For instance, to see the Reports menu, enter **R** at the prompt.

```
MM> R
                    REPORTS MENU

UNSR / UNLR    - User NI Short/Long Performance Report
UTSR / UTLR    - User TI Short/Long Performance Report
CNSR / CNLR    - Carrier NI Short/Long Performance Report
FESR / FELR    - Far End PRM Short/Long Performance Report
NSR:[z]        - User NI Statistical Performance Report
TSR:[z]        - User TI Statistical Performance Report
                 z = Display Report then Zero Counts (Optional)
AHR            - Alarm History Report
SHR            - Security History Report

PL:<len|style>- Set Page Length, <len> = 20 .. 70 (or 0 = Off), or
                <style> = P (Page Break), M (More), or V (View)

R>
```

DataSMART 658 only

DataSMART 658 only

Each time you change menus, the command-line prompt changes to indicate which menu is current. In the preceding figure, the first line shows a prompt of "MM>" meaning that the Main menu is current. However, once **R** is entered and the Reports menu is displayed, the prompt becomes "R>", indicating that the Reports menu is current.

The current menu displays when you press the Enter key. In normal use you are likely to use a series of commands from a given menu, and so you can make that menu current and get a menu listing whenever you need it by pressing the Enter key. However, you may enter any command at the command line, even if it is not on the "current" menu.

Command-line syntax

A typical command line consists of the command and zero or more arguments, all separated by one or more delimiters. The following are all valid delimiters: a space, a tab, a comma, a colon, a forward slash. You can use any combination of valid delimiters to separate arguments.

For example, **SD 12/08/97** and **SD 12 08 97** are both valid commands to set the date to December 8, 1997. However, SD 12-08-97 is not, because the dash is not a valid delimiter.

When entering an IP address or netmask, follow the dotted decimal convention (i.e., *nnn.nnn.nnn.nnn*) and include periods as part of this ID. The DataSMART will interpret the ID as a single argument.

There are two exceptions to these rules. One is a string value entered for the **SN, TCS**, **RCS**, **WCS**, **TPW**, **EPS**, **APS**, or **DPS** commands. In a string value, a space, comma, forward slash, or colon can appear in the argument, as long as there is a non-delimiter preceding it somewhere in the string. For example, this is a valid instance of the **SN** command:

SN PORTLAND, OR

The other exception is the syntax for logging into an DataSMART unit (see "Logging in" on page 25).

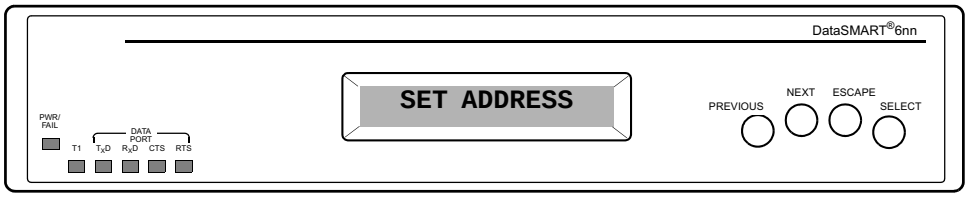
Type-ahead

You may enter the next command while a previous command is executing. The maximum type-ahead is three commands or 256 characters, whichever is less.

Using the front-panel interface

The front-panel interface is modeled after the command-line interface and provides most of the same functionality. The front-panel interface uses a hierarchical structure that you traverse using four push buttons on the front panel to find the command you need. The LCD display provides the visual readout.

Figure 3—The LCD display and push buttons



The hierarchical levels of the front-panel interface correspond to the menus, commands, and command options of the command-line interface. The Main menu at the top of the hierarchy corresponds to the Main menu of the command-line interface. Below that, depending on the complexity of the command, submenus correspond to the command menus of the command-line interface, then further subtrees allow you to select command options.

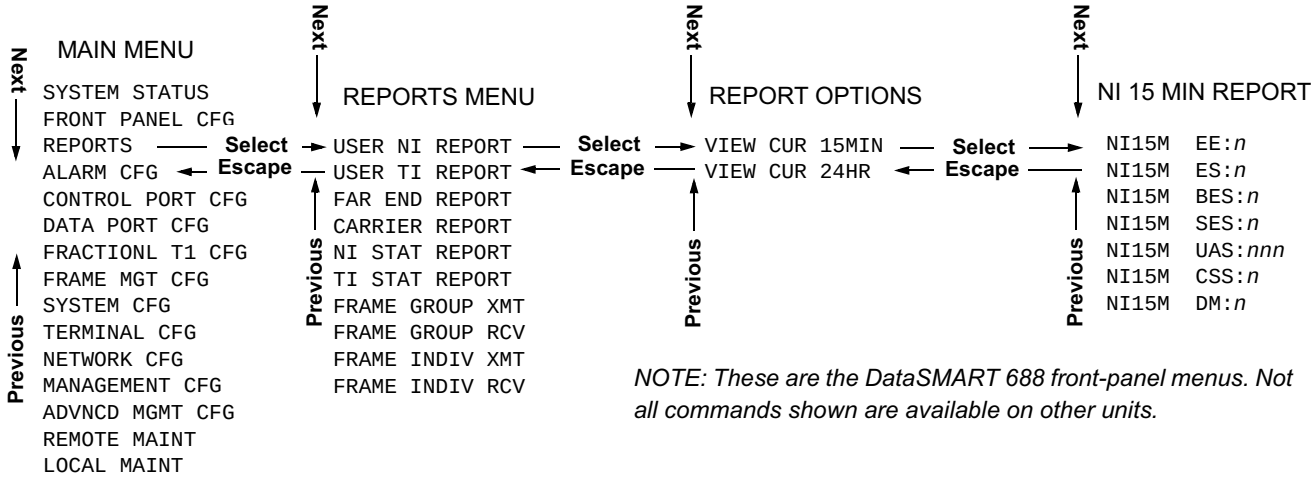
Traversing the hierarchy

The Select button moves you deeper into the hierarchy, the Escape button moves you back out towards the top. Next or Previous cycles you through all elements in one level of the hierarchy.

The figure on the next page illustrates these rules.

1. The Main menu is on the left side of the figure. Push Next or Previous to cycle through the items on the Main menu. When you see the item you want, push Select to descend to the next level, in this case the Reports menu.
2. In the Reports menu, push Next or Previous to cycle through the report choices. When you see the report you want, push Select to descend to the next level, the Report Options.
3. From the Report Options menu, choose to view either the report for the current 15 minutes or the current 24 hours; then push Select to descend to the first item in the report display.
4. As shown in the figure, the report display contains seven items that you can cycle

through using Next or Previous.

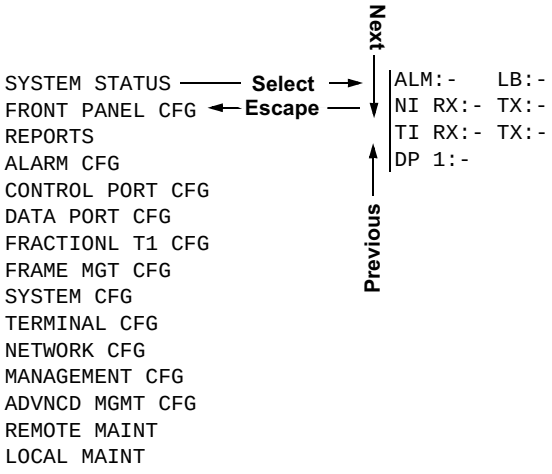


NOTE: These are the DataSMART 688 front-panel menus. Not all commands shown are available on other units.

Notice that you can "cycle" through items at each level in the hierarchy, and yet there is a conceptual "top" to each. Each level is circular in that pushing Next or Previous eventually brings you back to where you started. Each level has a "top" in that whenever you descend to a level by pushing Select, you always see the top item in the level. In the case of the Reports menu, the top item is USER NI REPORT.

However, when you use Escape to ascend from one level to the one above, you go back to the item that you originally descended from. For instance, if you entered the Report Options menu from FAR END REPORT, you would return to FAR END REPORT if you pushed Escape.

Not all hierarchies in the front-panel interface are as complex as the one in the last example. For instance, the simplest is for reading the System Status. In this case, when you see SYSTEM STATUS in the display, push Select. You can then use Next or Previous to cycle through the System Status display.



NOTE

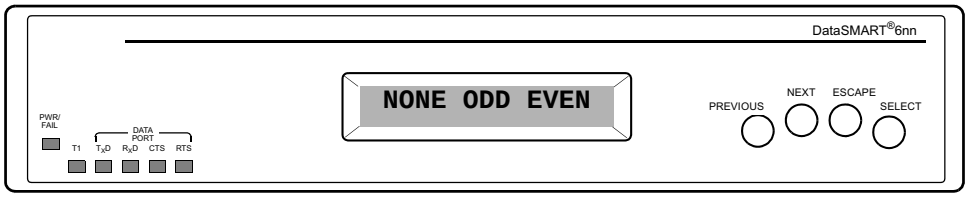
If you lose your place in the hierarchy, you can always return to a known point by pushing the Escape button until you see SYSTEM STATUS in the display; you will be back at the top of the Main menu.

Using the front panel for entering values

You can use the front panel for configuring ports, channels, and performing other operations that require you to enter values. There are three basic situations when entering values:

- Selecting from multiple choices displayed together in the panel
- Selecting multiple choices by cycling through a list
- Entering a string, IP address, or channel configuration

Selecting from multiple choices displayed together. The figure below illustrates choices displayed together: in this case, the parity setting for the control port.

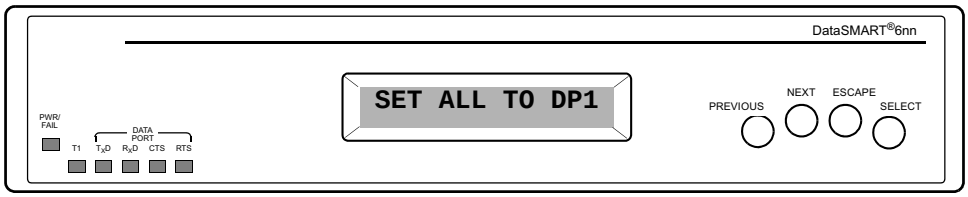


When the display appears, the current selection is blinking. To change to another value in the display, push Next or Previous. As you cycle through the selections, each will blink in turn.

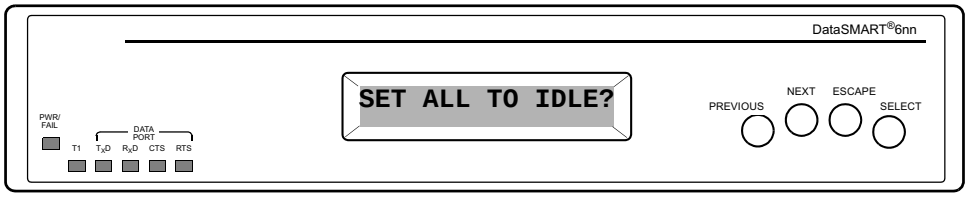
TIP
When you change a setting in the LCD display, a question mark appears indicating that a change to the DataSMART configuration is pending. Push Select to change to the configuration; push Escape to return the display to the original setting with no change to the configuration.

As soon as you change a selection in the display, a question mark appears on the right side of the display, indicating a change has been made in the display that has not yet been made to the DataSMART configuration. Push Select to make the change to the configuration and the question mark disappears (except in the case of entering a string, IP address, or channel configuration. See "Entering a string, IP address, or channel configuration" on page 15.)

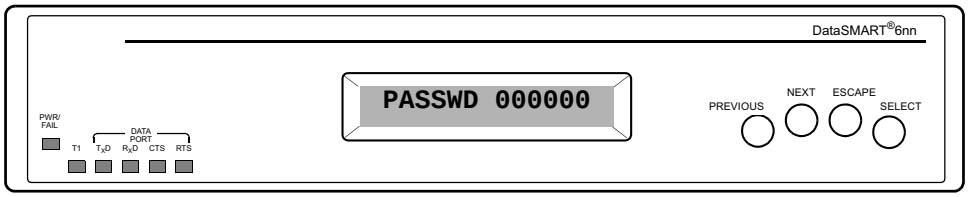
Selecting multiple choices by cycling through a list. In this case, you cannot see all your choices in the display. For example, the following figure shows a display for fractional T1 configuration. In the display, "DP1" blinks to indicate that it is the current selection and can be changed.



Pushing Next changes the selection to "IDLE" as shown below. The question mark indicates that a change to the configuration is pending. If you push Select now, IDLE will become the current configuration.



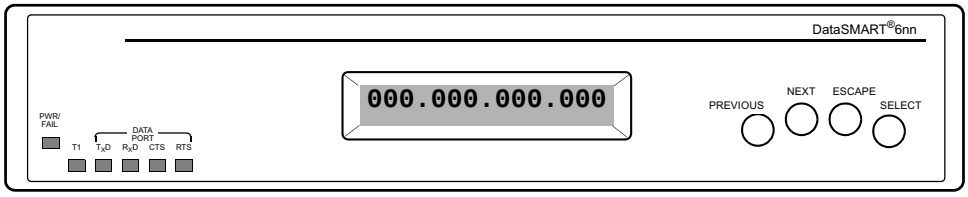
Entering a string, IP address, or channel configuration. The figure below illustrates the display for changing the front-panel password. As the figure shows, a password is a string of six numerals.



When the display first comes up, the first numeral is underlined. Pushing Next or Previous moves the underline to a different numeral. To change the underlined numeral, push Select. The underline disappears and the numeral begins blinking. When the numeral is blinking, push Next or Previous to change the numeral.

As soon as you change the numeral in the display, a question mark appears to the right, indicating that you have changed a value in the display but have not yet changed the value in the DataSMART configuration. Push Select to make the change to the configuration. The numeral stops blinking, the question mark disappears, and the underline reappears. You can now use Next or Previous to move the underline to a different numeral for further editing. If you push Escape when the question mark is showing, the numeral returns to its original setting.

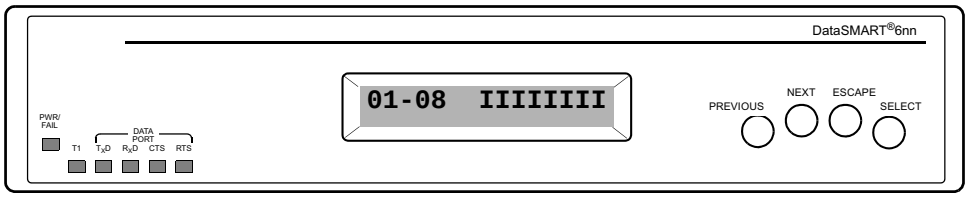
Entering an address works similarly, though with some differences worth noting. For instance, the following figure shows the display for setting the IP address. In this case, Next or Previous moves the underline between the fields rather than stopping at each numeral. You use the same procedure to change the fields as for changing the numerals of a password.



The question mark appears each time you edit a field, and disappears when you push Select. However, the changes you make in the display do not take effect in the DataSMART configuration until you leave the IP address display. In other words, after you make all the changes to the fields (pushing Select after each one), you must push Escape. The query SET NEW ADDRESS? appears in the display. If you push Select, the changes are made to the configuration. If you push Escape, the changes you made in the display are discarded.

The process for entering channel configurations has similarities to both entering strings and entering addresses.

The following figure shows the initial channel configuration display. The display shows the settings for channels one through eight, which in this case are all set to idle, as indicated by an “I” for each channel.



When you first enter the display, the channel range is blinking. If you push Next or Previous at this point, the ranges will cycle through “01- 08,” “09-16,” and “17 - 24.” When you see the range you want to edit, push Select. The range will stop blinking, and an underline will appear under the token representing the first channel.

At this point, you change the token just as you would change a numeral in the password string. Push Select, and the token begins blinking, then push Next or Previous to change the token. The question mark appears when you change the token. When you have changed the token to the one you want, push Select; the question mark disappears and the underline reappears. You can then use Next or Previous to move the underline to the next token you wish to change.

Once all the channels for the range are correctly set, push Escape. The range begins blinking and you can change to the next range. When all the channels are set correctly, push Escape to exit the channel configuration display. The query “LOAD NEW CHANS?” appears. Push Select to load the new channel configuration into the hardware or push Escape to discard the changes.

Logging in

You can log into a DataSMART unit using an ASCII connection to the control port; using IP access through a control port; or by using ARC to connect to a remote unit over the facility data link. Passwords are not needed, but, when implemented, can restrict some users from using some commands.

The DataSMART can be accessed through a number of methods:

- Using the command-line interface over an ASCII connection to the unit's DCE or DTE control port
- Using the command-line interface over an IP connection (Telnet) to the Ethernet port
- Using the command-line interface over an IP connection (Telnet) to the control port, configured for PPP or SLIP
- Using the command-line interface over an IP connection (Telnet) over the facility data link or DS0 data link within the T1 data stream
- Using the command-line interface and ARC over the Facility Data Link (FDL)
- Using the front-panel LCD interface
- Using an SNMP network manager over an IP connection

In general, a password is not needed to log into a DataSMART unit. Though DataSMART units support passwords, the passwords do not prevent login but instead restrict users from executing various commands. (See Chapter 3 for procedures on setting passwords.)

Depending on whether you are accessing the DataSMART through Telnet, the facility data link, a DS0 channel, or the DTE or DCE control port, the procedure for logging in differs.

Through the control port (single unit) via ASCII

On a single unit, the device typically has the address of 00:00:000. In this case, simply press the Enter key to log in. The DataSMART unit will display the Main menu and the command prompt, indicating you are logged in.

Through the control port (daisy-chain) via ASCII

When units are daisy-chained, each unit must have a unique address. The command syntax to log into a daisy-chained unit is:

^D*xx*:*yy*:*zzz***^E**

where

^D, ^E Press the Ctrl and D (or Ctrl and E) keys simultaneously.

xx:*yy*:*zzz* is the address of the unit you want to log into.

When you log in using the syntax **^D***xx*:*yy*:*zzz***^E** you see the full Main menu.

Note that the colon is the only valid delimiter for the login command.

Through the facility data link

The facility data link (FDL) uses a signal embedded in the T1 framing pattern to enable you to log into a remote DataSMART DSU on the far end of a T1 line. The FDL is available only if the two units are both using Extended Super Frame (ESF) framing.

You must be logged into the near-end DataSMART DSU before you can access a far-end unit. Once you are logged into the near-end DataSMART DSU, enter this command:

ARC

The angle brackets in the command prompt change from ">" to "<" to indicate that you are logged into a far-end device. For example, the ARC Main menu prompt is "MM<".

You log out of the far-end device by entering this command:

DRC

Telnet access

If your DataSMART unit has been configured for IP access and you have set up a Telnet password on the unit, you can log into it using Telnet. When you enter the unit's IP address and attempt to log in, you will be prompted for its Telnet password. If the DataSMART has not been set up for IP access and assigned a Telnet password, you will not be able to log in.

See Chapter 8 for information on configuring a DataSMART unit for Telnet login.

Logging out

You should always log out of the DataSMART when you are done.

To log out, enter **^D**. (Press the Ctrl and D keys simultaneously.)

If you have logged into a remote DataSMART using **ARC**, use the **DRC** command or **^D** to log out.

You can also log out by disconnecting the control port cable.

The DataSMART has an auto-logout feature that logs you out after a period of inactivity. Auto-logout is always enabled when Telnet or ARC is being used. If auto-logout was disabled before a Telnet session is started, auto-logout is set to 15 minutes for that Telnet session. When the user logs out, auto-logout reverts to the default configuration value. If auto-logout is enabled before a Telnet session is started, the auto-logout time will not be changed. See "Setting auto-logout for the control port" on page 48.

CHAPTER

3 *Establishing system security*

In order to prevent unauthorized users from changing the system configuration, setting loopbacks, or performing other operations that might disrupt service, you need to secure access to the user interfaces.

This chapter show you how to secure access to:

- The command-line interface via the control port
- The front-panel interface via the LCD and push-buttons

The SNMP and Telnet security features are discussed elsewhere in this manual. For information about securing SNMP access, see “Setting SNMP community strings” on page 190 and“Using SNMP traps” on page 196 . For information about securing the Telnet password, see “Setting the Telnet password” on page 182.

Securing the command-line interface

Security for the command-line interface is achieved through a system of passwords and privilege levels. Any user can access the command line without entering a password. But in order to gain a specific privilege level, the user must enter a password that has that privilege level assigned to it.

Restricting access

By default, there are no restrictions on which commands you can run on the DataSMART. Every user has super-user privileges. In order to restrict access, you must create at least one password with the super-user privilege level. Once you do, every user is restricted to the read-only privilege level unless they enter a password that permits more extensive privileges. You may create up to ten passwords (assuming you have super-user privileges) and assign them any privilege level you like.

NOTE

If you do not create a password with a super-user privilege level, every user that accesses the command line will be granted super-user privileges, regardless of whether or not you have created passwords for the other privilege levels.

Table 1—Privilege levels

Privilege level	Description
Read-only	Users with no password, and thus no privilege level, have read-only access. They can view menus, status screens, and performance reports, but they cannot execute any diagnostics nor change any configuration options.
Maintenance	Users with this privilege level can execute diagnostic tests, such as loopbacks and BERTs. Their activities can potentially disrupt data traffic through the device.
Configuration	Users with this privilege level can execute all tests allowed at the Maintenance level, plus they can change the configuration options of the DataSMART. Their activities can potentially disrupt service to the device.
Super user	Users with this privilege level have access to all commands allowed at the Configuration level, plus they have access to the commands that set up and control passwords.

The commands available for setting up and controlling command-line passwords are listed in the Password Entry and Configuration menu. To display this menu, log into the desired unit, then enter **PC** at the command line.

```
          PASSWORD ENTRY AND CONFIGURATION MENU

 EPS:<password>          - Enter Password
                           password = 6 to 12 characters

 APS:<access>:<password> - Add Password
                           access   = SA - Super User
                                      CA - Configuration
                                      MA - Maintenance
                           password = 6 to 12 characters

 DPS:<password>          - Delete Password
                           password = 6 to 12 characters, or * for all

 PUV                     - View User Access Privilege
 PCV                     - View Password Configuration
```

Adding a password

You create a new password by using the **APS** command. You must have super-user privileges. The command syntax is:

APS:*access***:***password*

access — Specify the privilege level you want linked to the password: **SA** (super user), **CA** (configuration), or **MA** (maintenance).

password — Specify the password you want added. The string can comprise from six to twelve ASCII printable characters. (If the string you enter is either too long or too short, you'll get an error message.) Passwords are not case-sensitive and trailing spaces are not truncated.

Up to ten passwords are allowed. If you attempt to enter an eleventh password, you will get an error message. To add another password, you must first delete an existing password.

Each password must be unique.

Deleting a password

You delete a password using the **DPS** command. You must have super-user privileges. The command syntax is:

DPS:*password*

password — Specify the password you want deleted. The string must match the password exactly, except for case. You can also enter the * wild-card character to delete all current passwords.

Entering a password

To gain the privilege level associated with a password, use the **EPS** command. No special privileges are required. The command syntax is:

EPS:*password*

password Enter the password. Passwords are not case-sensitive.

If you enter the password correctly, DataSMART responds with the message PASSWORD ACCEPTED. If you enter an incorrect password, it responds with the message PASSWORD DENIED.

Viewing a user's access level

If you are logged into the device, you can view your privilege level by using the **PUV** command. You do not need any special privilege level. You will receive one of the following messages:

"User has No Access Privileges"
"User has MA Access Privileges" (maintenance)
"User has CA Access Privileges" (configuration)
"User has SA Access Privileges" (super user)

If your password was modified during your current session (e.g., a super user deleted your password, then added it back with a different privilege level), the change will not become effective until the next time you specify the password with the **EPS** command.

Changes to a user's password or privilege level take effect only after the user has logged out.

Viewing the current passwords

You can view a listing of current passwords and their privilege levels using the **PCV** command. You must have super-user privileges.

An example listing is shown below. The left column lists the current passwords, the right column identifies the access privilege levels.

```
        VIEW PASSWORD CONFIGURATION

Password      Access
------------  ------
BROWNS        MA
JOHNSOND      CA
MITCHELLS     SA
```

Securing the front panel

After you have installed the DataSMART and are controlling it remotely, you may want to disable the front-panel LCD and push buttons. Disabling the front panel prevents unauthorized or careless users from changing the DataSMART configuration and disrupting service.

A disabled front panel can be used for examining status, performance, and configuration, but not for changing any parameters. One way to think of it is that a disabled front panel is in “read-only mode” while an enabled front panel is in “read/write mode.”

There are two approaches to disabling the front panel. You can disable the front panel without setting a front-panel password, or you can set a password and disable it.

If you do not set a password, any user can disable, then re-enable the front panel. This provides minimum security for times when you want to temporarily disable configuration access. For example, you might want to secure the front panel this way while you are viewing status, since this would prevent you from inadvertently changing a parameter while pushing buttons. However, for full security, you want to set a password. If you set a password, only users who enter the password can re-enable the front panel once it has been disabled. The front panel can also be re-enabled by entering **EFP** via the command line interface.

Using auto-logout

Another benefit to setting a front-panel password is that you can employ the front-panel auto-logout feature. This feature automatically disables the front panel if there has been no user activity at the front panel for a specified period of time. The information displayed on the front panel then changes to a readout of %EFS (percentage error-free seconds) when the auto-logout occurs. The next user needs to enter the password to re-enable the front panel.

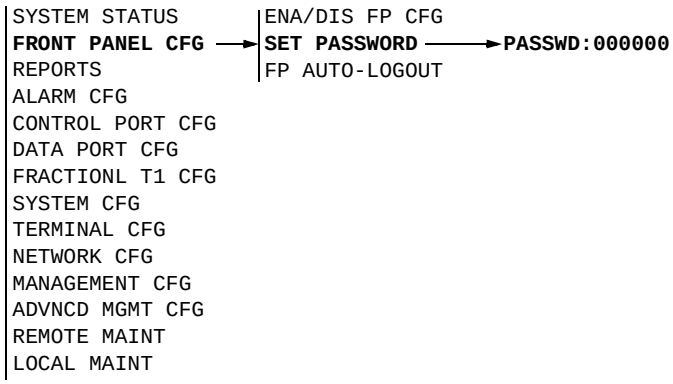
If a password has not been defined for the front panel, the auto-logout feature has no effect except to show the %EFS display.

Setting the front-panel password

To set the front-panel password, use the steps shown below. The password is six digits. All zeroes is the equivalent of "no password." Note that if the front panel is disabled, instead of seeing SET PASSWORD in the display, you will see ENTER PASSWORD.

The default password is 000000 (no password).

The password is stored in the permanent nonvolatile configuration database.

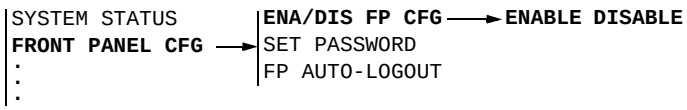


1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until FRONT PANEL CFG appears in the display.
3. Push Select. ENA/DIS FP CFG appears in the display.
4. Push Next or Previous until SET PASSWORD appears in the display.
5. Push Select. PASSWD:0̲00000 appears in the display.
6. Push Next or Previous to move the underline marker to the digit field you want to change.
7. Push Select. The digit will blink.
8. Use Next or Previous to change the digit value.
9. When the digit is set to the value you want, push Select. The message PASSWD SET indicates that the password has been changed.
10. Repeat steps 6 through 9 to change the rest of the digits as desired.

Enabling/disabling the front panel

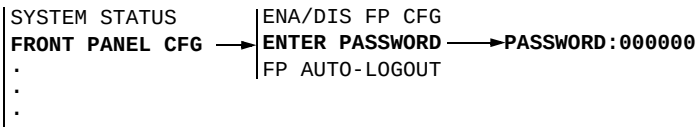
The default state for the front panel is enabled. The setting is stored in the permanent nonvolatile configuration database.

To enable or disable the front panel when no password is set, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until FRONT PANEL CFG appears in the display.
3. Push Select. ENA/DIS FP CFG appears in the display.
4. Push Select. ENABLE DISABLE appears in the display, with the current selection blinking.
5. Push Next or Previous to choose the desired selection.
6. Push Select.

To enable the front panel when a password is set, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until FRONT PANEL CFG appears in the display.
3. Push Select. ENA/DIS FP CFG appears in the display.
4. Push Next or Previous until ENTER PASSWORD appears in the display.
5. Push Select. PASSWD:000000 appears in the display.
6. Push Next or Previous to move the underline marker to the appropriate digit field.
7. Push Select. The digit will blink.
8. Use Next or Previous to specify the appropriate digit.
9. Push Select.
10. Repeat steps 6 through 9 to change the rest of the digits to the correct password. When the password is correct, PASSWD ACCEPTED appears in the display.

Using the command line

You can also enable or disable the front panel from the command-line interface by using the **EFP** and **DFP** commands, respectively. You must have super-user or configuration privileges.

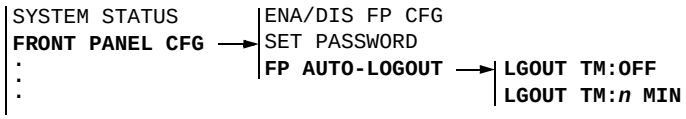
EFP	Enable the front panel.
DFP	Disable the front panel.

Setting auto-logout for the front panel

You can set the auto-logout timer to OFF (disabled), or from 1 to 60 minutes, inclusive. Use the steps shown below.

The default for auto-logout is OFF.

The auto-logout setting is stored in the permanent nonvolatile configuration database.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until FRONT PANEL CFG appears in the display.
3. Push Select. ENA/DIS FP CFG appears in the display.
4. Push Next or Previous until FP AUTO-LOGOUT appears in the display.
5. Push Select. The current auto-logout setting appears: OFF or a value from 1 to 60.
6. Push Next or Previous to change the timer value, then push Select.

CHAPTER

4 *Configuring the system*

This chapter discusses configuration operations that apply to the DataSMART as a whole. It covers the commands and options listed in the System Configuration, Control Port Configuration, and Alarm Configuration menus.

Topics include:

- Setting the DataSMART real-time clock and source clock
- Resetting the DataSMART unit to its default state
- Configuring the control port
- Configuring alarm message output
- Specifying error thresholds for reporting

For information on configuring interface ports and assigning channels, see Chapter 5.

For information on configuring the DataSMART for network management, see Chapter 8.

Specifying system parameters

You can control the system-level parameters and activities by using the command-line interface or the front-panel interface.

Command-line access

The commands for configuring the system parameters are listed below. To display this menu, first log into the unit, then enter **SC**.

```
                    SYSTEM CONFIGURATION MENU

SD:<mm>,<dd>,<yy>          - Set Date (Warning: This also clears reports)
ST:<hh>,<mm>               - Set Time (Warning: This also clears reports)
SN:<id>                    - Set Name
SA:<xx>,<yy>,<zzz>         - Set the Unit's Address to slot:shelf:group
EFP / DFP                  - Enable/Disable Front Panel Operation
EDC / DDC                  - Enable/Disable DataSMART Compatibility
CLK:<src>                  - Clock Source, src = L (Loop), C (CSU Thru)
                             T (TI Receive), I (Internal), 1 (DP1)
ALGOUT:<n>                 - Autologout, n = 0 .. 60 minutes
ZALL                       - Zero All Counters used in User Reports
TSWDL:<i>                  - Download program from a file via TFTP
                             i = n.n.n.n, n = 0..255 (dec), the
                                 IP address of the TFTP host system
BOOT:<b>                   - Re-boot the system
                             b = A (Active FLASH) or I (Inactive FLASH)
WYV                        - View "What's Your Version" Information
RSD                        - Reset System to Default Values
SCV                        - View System Configuration
```

C, T available on add/drop only

Front-panel access

The front-panel commands for configuring the system are as follows.

```
SYSTEM STATUS
FRONT PANEL CFG
REPORTS
ALARM CFG
CONTROL PORT CFG
DATA PORT CFG
FRACTIONL T1 CFG
SYSTEM CFG  ------>  SET DATE
NETWORK CFG          SET TIME
MANAGEMENT CFG       SET NAME
ADVNCD MGMT CFG      SET ADDRESS
REMOTE MAINT         DATASMART COMPAT
LOCAL MAINT          CLOCK SOURCE
                     AUTO-LOGOUT TIME
                     ZERO COUNTERS
                     VERSION INFO
                     RESET DEFAULTS
```

Viewing the current settings

Before changing any system parameters, you may want to look at the current settings. You do this by executing the **SCV** command. This command displays the View System Configuration screen.

```
        VIEW SYSTEM CONFIGURATION

Date          Time   Name             Address    Autologout
------------  -----  ---------------  ---------  ----------
JAN 11, 1997  14:10  PORTLAND,OR      01:00:000  DISABLED

User Clock   Current Clock  Front Panel  ARC Mode
-----------  -------------  -----------  ---------------
LOOP         LOOP           ENABLED      DS 72xxx/MPATH
```

Field	Description
Date	This field displays the current date of the real-time clock.
Time	This field displays the current time of the real-time clock.
Name	This field displays the name assigned to the DataSMART unit you are logged into. The name appears in the Main menu, in all performance reports, and in alarm messages. It is also the name returned for the MIB II *sysName* object.
Address	This field displays the physical (daisy-chain) address of the DataSMART unit you are logged into. The address is in the form of *xx*:*yy*:*zzz*, where *xx* corresponds to slot location, *yy* is the shelf address, and *zzz* is the group address.
Autologout	This field specifies the state of auto-logout. If auto-logout is enabled, it displays the auto-logout period in minutes.
User Clock	This field identifies the clock source you have assigned to be used as the system clock.
Current Clock	This field tells you the *actual* clock source being used as the system clock. Under normal operating conditions, this field will be identical to the "User Clock." If the unit loses its assigned clock, it switches to its internal clock.
Front Panel	This field tells you if the front panel is currently enabled or disabled.
Compatibility (ARC Mode)	This field tells you what kind of units you can log into via ARC. The choices are: DS 72xxx/MPATH (default): Compatible with DataSMART 72000 series DSU/CSU (including SPort and MAX) or M-PATH CSUs. DataSMART 78xxx: Compatible with DataSMART 78000 series DSUs including the DataSMART Single Port DSU.

Setting date and time

The DataSMART uses an internal, real-time clock to time stamp event occurrences. The time stamps appear in alarm messages and performance reports as an aid to troubleshooting. To make the time stamps accurate, you must set the date and time of the real-time clock upon system installation.

Once you have set the real-time clock, you need to reset it only if the DataSMART has an extended power loss. The real-time clock operates for two hours, nominally, after power is lost.

CAUTION!
When you change the date or time parameters of the real-time clock, all performance data is cleared from all reports.

Using the command line

Set the date by using the **SD** command. You must have super-user or configuration privileges. The command syntax is:

SD:*mm*,*dd*,*yy*

mm	Specify the month. You can enter the three-letter abbreviation or the number of the month.
dd	Specify the day of the month. The DataSMART performs a range check on the entered value to see if the day is valid for the given month and year.
yy	Specify the last two digits of the year between 1992 and 2091.

TIP
If you want to track between Daylight Savings Time and Standard Time, you will need to reset the "time" parameter when local time changes.

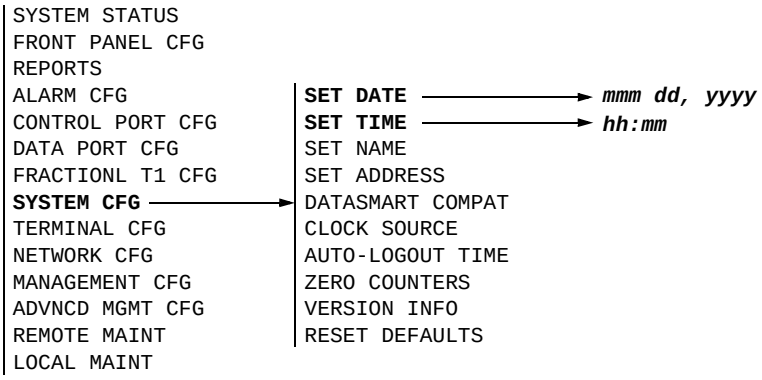
Set the time by using the **ST** command. You must have super-user or configuration privileges. The command syntax is:

ST:*hh*,*mm*

hh	Specify the hour. The time is specified in "24-hour" format, where 12:00 is noon and 00:00 is midnight. Allowed values are 0 to 23, inclusive.
mm	Specify the minutes. Allowed values are 0 to 59, inclusive.

Using the front panel

To set the date and time from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until SYSTEM CFG appears in the display.
3. Push Select. SET DATE appears in the display.
4. If you want to change the date, push Select. A string showing the date appears in the display.

   If you want to change the time, push Next or Previous until SET TIME appears in the display, then push Select. A string showing the current time appears in the display.
5. The SET DATE and SET TIME strings are divided into fields. To select a field to change, push Next or Previous until the field is underlined, then push Select.
6. Push Next or Previous to cycle through the allowed field values.
7. When the value you want is displayed, push Select. The LCD displays CLR PERF DATA? to remind you that changing the date or time clears performance data from the performance reports. Push Select again to change the date or time, or push Escape to abort. If you push Select, PERF DATA CLEARD appears on the screen, indicating that the date or time has been reset and the performance data cleared.
8. Repeat steps 4 through 7 to change each field in the date or time string.

Naming the device

Each DataSMART is assigned a device name that appears in alarm messages, performance reports, and at the top of the Main menu. You can specify any name up to 15 characters long. Usually the name represents your site or the service you are connected to.

The device name specified here is also the name returned with the MIB II *sysName* object.

The default device name is "PORTLAND,OR."

Using the command line

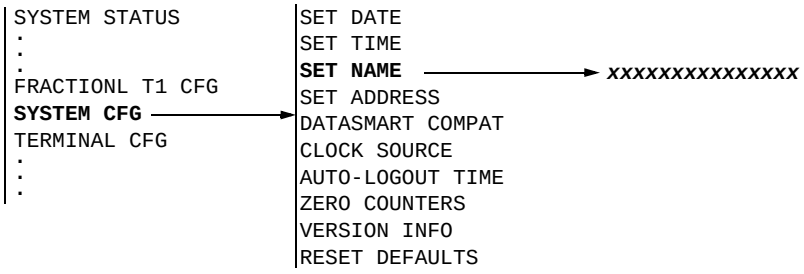
You change the device name by using the **SN** command. You must have super-user or configuration privileges. The command syntax is:

SN:*id*

id	Enter the device name. The name can be up to 15 characters long, including spaces, commas, or colons. A space, comma, or colon may not appear in the first position. Trailing spaces are truncated. Alphabetic characters are saved as upper case.

Using the front panel

A name entered via the front panel can be 15 characters long. To set the name from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until SYSTEM CFG appears in the display.
3. Push Select. SET DATE appears in the display.
4. Push Next or Previous until SET NAME appears in the display.
5. Push Select. The current device name appears in the display.
6. Push Next or Previous to select the character in the field you want to change. When the character field you want to change is underlined, push Select.
7. Push Next or Previous to change the character. When the character you want is displayed, push Select.
8. Repeat steps 6 and 7 until you have changed all the character fields you want.
9. Push Escape. SET NEW STRING? appears in the display. Push Select or push Escape to abort.

Specifying an address

When multiple DataSMART units are configured in a daisy-chain, you must assign each a unique address. A daisy-chain allows you to log into multiple DataSMART units through one control port—that way you do not need a separate terminal for each DataSMART. The unique address makes it possible for you to specify which DataSMART in the daisy chain you want to log into.

TIP
The device address is not the same as the IP address. See "Setting the IP address" on page 179 for instructions on setting the IP address.

Typically you will connect the DataSMART units into a daisy chain and then use the front panel to assign addresses to each one. However, it is possible to assign an address from the command line.

The default device address is 00:00:000. Do not change the address unless you are putting the DataSMART in a daisy chain.

The device address is stored in the permanent nonvolatile configuration database.

Using the command line

To set the device address, use the **SA** command. You must have super-user or configuration privileges. The syntax for the command is:

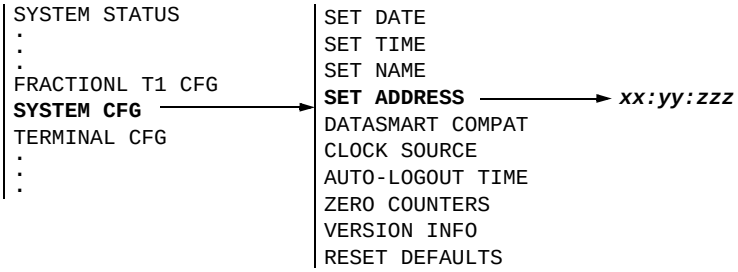
SA:*xx***,***yy***,***zzz*

The allowed values for the three address fields are:

xx = 0 - 15
yy = 0 - 15
zzz = 0 - 255

Using the front panel

To set the device address from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until SYSTEM CFG appears in the display.
3. Push Select. SET DATE appears in the display.
4. Push Next or Previous until SET ADDRESS appears in the display.
5. Push Select. The current address appears in the display.
6. Push Next or Previous to move between address fields. When the field you want to change is underlined, push Select.
7. Push Next or Previous to change the value in the field. When the value you want is displayed, push Select or push Escape to abort.
8. Repeat steps 6 and 7 until the address fields are correct.

Logging in with an address

You do not need to log into a stand-alone device with an address of 00:00:000. Simply press the Enter key on your terminal, then enter your password (if passwords have been established).

To log into a device in a daisy chain, enter:

^D*xx*:*yy*:*zzz***^E**

where

^D, ^E Press the Ctrl and D (or Ctrl and E) keys simultaneously.

xx:*yy*:*zzz* is the address of the unit you want to log into.

Note that the colon is the only valid delimiter for the login command.

When you log in using the syntax: **^D***xx*:*yy*:*zzz***^E** you see the Main menu.

To log out of a device, enter:

^D

Enabling/disabling the front panel

To secure the front panel, you need to set a front-panel password, then enable or disable the front-panel push buttons as desired. For more information, see "Securing the front panel" on page 31.

Specifying DataSMART compatibility

You can choose whether to make ARC remote login capability compatible with older DataSMART units or newer units.

Using the command line

Use the **EDC** and **DDC** commands to set ARC mode compatibility.

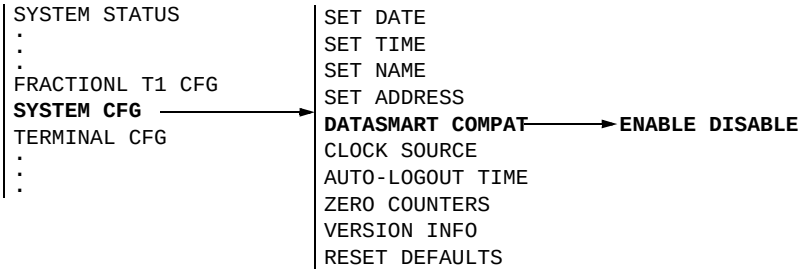
DDC Allows ARC communications with DataSMART 500 and 600 series units, DataSMART MAX/SPort and M-PATH CSUs.

EDC Allows ARC communications with DataSMART 78000 series DSUs such as the DataSMART Single Port.

DDC is the default. See "Commands available via ARC" on page 212 for more information.

Using the front panel

To set the device address from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until SYSTEM CFG appears in the display.
3. Push Select. SET DATE appears in the display.
4. Push Next or Previous until DATASMART COMPAT appears in the display.
5. Push Select. ENABLE DISABLE appears in the display with the current selection blinking.
6. Push Next or Previous to change the selection. When the desired choice is blinking, push Select.

Specifying the system clock

The DataSMART times all outputs using one signal. For most applications, the DataSMART is set to derive its source clock from the network receive signal (Loop Timing). This is the most common timing setup and should be used if your T1 service provider supplies timing. If your T1 service provider does not supply timing, you must select an alternate source as specified in Table 3.

Figure 4 on page 46 illustrates some common timing applications. When setting up your T1 circuit timing, it is important to remember this general rule: **There must be one and only one timing source for the T1 circuit**.

The default is Loop Timing (i.e., the network receive signal).

Table 2—Timing options

Timing option	Description
Loop Timing (**L**)	This option tells the DataSMART to derive its system clock from the incoming signal at the network interface. Select this option if: 1) the T1 service provider is supplying a timing source, or 2) you are using the far-end device in a point-to-point connection as the master timing source.
CSU Through Timing (**C**) (658 only)	This option times data output by passing through the timing with the data. The timing signal passes through transparently. Do not select the CSU Through Timing option if you want to assign any DS0 channels to the DataSMART unit's data port.
TI Receive Timing (**T**) (658 only)	This option tells the DataSMART to derive its system clock from the incoming signal at the terminal interface. Select this option if: 1) the T1 service provider is not supplying a timing source, and 2) you want to receive timing from a device beyond the terminal interface, such as a PBX.
Internal Master Timing (uppercase **I**)	This option tells the DataSMART to use its internal oscillator as the system clock. In this case, the DataSMART becomes the master in a point-to-point connection. The far-end device should use Loop Timing. Select this option only if the T1 service provider is not supplying a timing source.
Data Port 1 Timing (numeric **1**) (This is also known as Tail Circuit Timing)	This option tells the DataSMART to derive its system clock from the signal being received on the data port connector's external clock pins (see Table 17 on page 221). The data port configuration must be set to the data rate received and the clock supplied must meet the network accuracy standard of ±32 ppm. Select this option only if the T1 service provider is not supplying a timing source and the timing source is the device connected to the specified data port. To use this option, at least one DS0 channel must be assigned to the data port. However, data port timing is not available if the IP management data link is using a channel assigned to the data port.

Secondary clock source

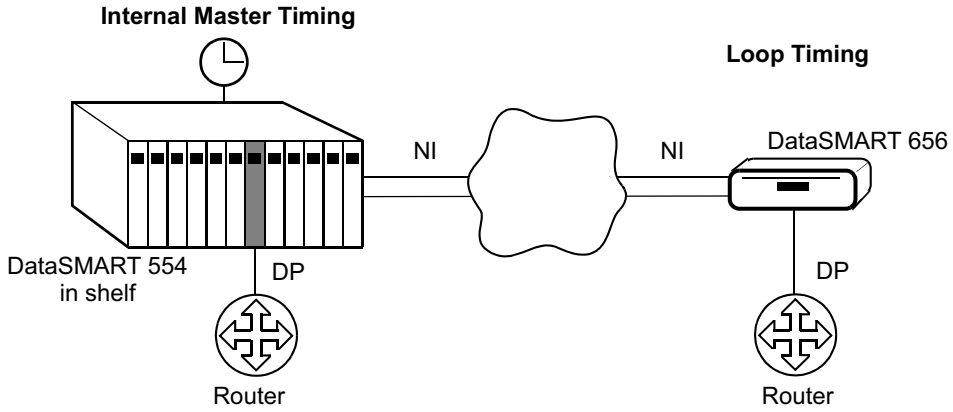
If the expected timing source is not present or is lost, the DataSMART defaults to Internal Master Timing. This occurs under the conditions specified in Table 3.

Table 3—Conditions that cause a default to internal timing

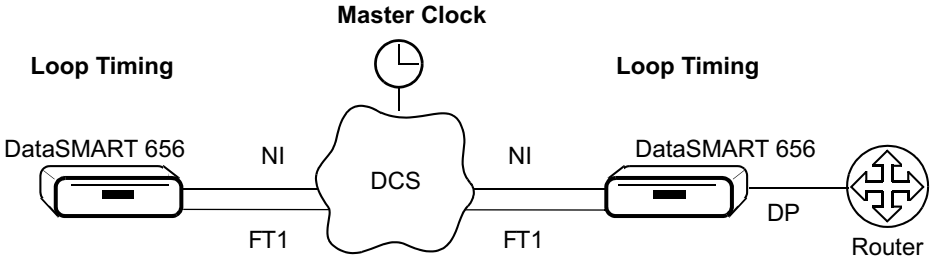
Timing option	Condition
Loop Timing	The DataSMART defaults to internal timing if it cannot detect a framed incoming signal at the network interface, either because the signal is lost or because the signal is out of frame or AIS is detected.
CSU Through Timing (add/drop only)	If the DataSMART cannot detect a framed signal at the network interface or terminal interface, it sends a "keep alive" signal and also defaults to internal timing. This happens when the signal is lost or because the signal is out of frame or AIS is detected. For the format of the "keep alive" signal, see"Specify the "keep alive" signal for the network interface (add/drop units only)" on page 78.
TI Receive Timing (add/drop only)	The DataSMART defaults to internal timing if it cannot detect a clock in the incoming signal at the terminal interface, either because the signal is lost or because the signal is out of frame or AIS is detected.
Data Port Timing	The DataSMART defaults to internal timing if it cannot detect an XCLK signal at the data port, either because a clock signal is not present or because a DPLOS has occurred.

Figure 4—Common timing applications

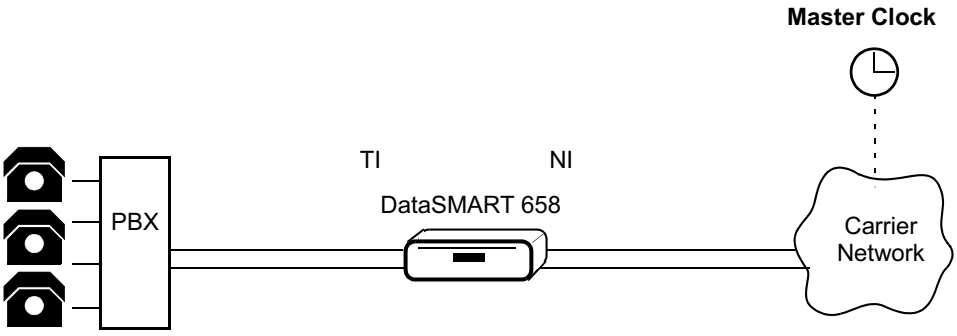
POINT-TO-POINT DSU/CSU APPLICATION: SPAN UNTIMED



FRACTIONAL T1 DSU/CSU APPLICATION: SPAN TIMED BY CARRIER



CSU APPLICATION: CSU THROUGH TIMING



Setting the clock source using the command line

You set the DataSMART source clock by using the **CLK** command. You must have super-user or configuration privileges. The command syntax is:

CLK:*src*

The *src* value specifies the source clock as:

C, T available on add/drop only

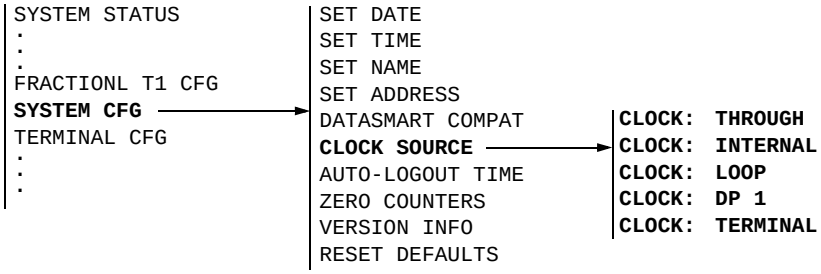
L	Loop Timing
C	CSU Through Timing
T	TI Receive Timing
I	Internal Master Timing
1	Data Port Timing (also known as Tail Circuit Timing)

NOTE

Be careful not to confuse uppercase I (for Internal timing) with numeric 1 (for Data Port 1 timing).

Setting the clock source using the front panel

To specify the clock source from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until SYSTEM CFG appears in the display.
3. Push Select. SET DATE appears in the display.
4. Push Next or Previous until CLOCK SOURCE appears in the display.
5. Push Select. The current clock setting appears in the display.
6. Push Next or Previous to cycle through the clock options. When the option you want appears in the display, push Select or push Escape to abort.

Setting auto-logout for the control port

You can program the DataSMART to automatically log out a user who has been inactive for a specified period of time. This feature helps prevent situations where:

- A user with a high privilege level forgets to log out, leaving the system open to unauthorized users
- A user forgets to log out and blocks other users from logging in
- A Telnet or ARC connection breaks down and hangs the connection

You can specify an auto-logout of 0 (off), or from 1 to 60 minutes, inclusive. A setting of 0 disables the auto-logout timer for users who log in via a serial device connected to the control port. It does not disable the timer for users who log in via Telnet or ARC—you cannot disable auto-logout for these types of remote logins. When the timer is set to 0, the DataSMART defaults to a 15-minute auto-logout period for Telnet or ARC.

The default for auto-logout is 0 (off).

Using the command line

To specify an auto-logout period for the control port, use the **ALGOUT** command. When you set the timer to a value greater than 0, that value is used as the auto-logout period for the control port, and for Telnet and ARC logins.

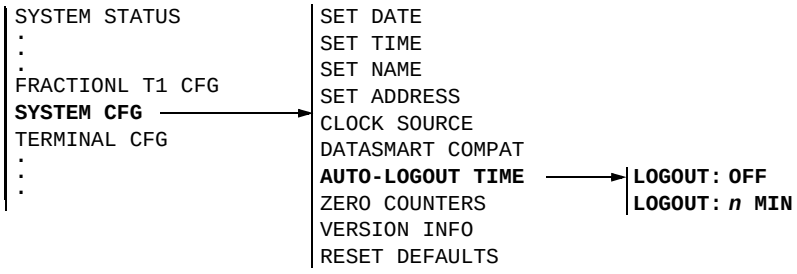
You must have super-user or configuration privileges to use the **ALGOUT** command. The command syntax is:

ALGOUT:*n*

n	Specify the auto-logout period in minutes, from 1 to 60, inclusive. 0 disables the timer (the auto-logout period for Telnet and ARC logins becomes 15 minutes).

Using the front panel

To specify an auto-logout for the control port from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until SYSTEM CFG appears in the display
3. Push Select. SET DATE appears in the display.
4. Push Next or Previous until AUTO-LOGOUT TIME appears in the display.
5. Push Select. The current timer setting appears in the display.
6. Push Next or Previous to cycle through the timer options: 1 - 60, or OFF. When the option you want appears in the display, push Select or push Escape to abort.

Setting auto-logout for the front panel

The front-panel auto-logout feature prevents you from inadvertently leaving the front panel in an enabled state. See "Securing the front panel" on page 31 for more information.

Zeroing all counters

If you change the configuration parameters for the DataSMART, you may want to clear the performance database. You do this by zeroing all counters. This clears the data from the following:

- User NI Short and Long Performance reports
- User TI Short and Long Performance reports (658 only)
- Far-end PRM Short and Long Performance reports
- User NI Statistical Performance report
- User TI Statistical Performance report (658 only)
- Error threshold counters

It does not clear the data from:

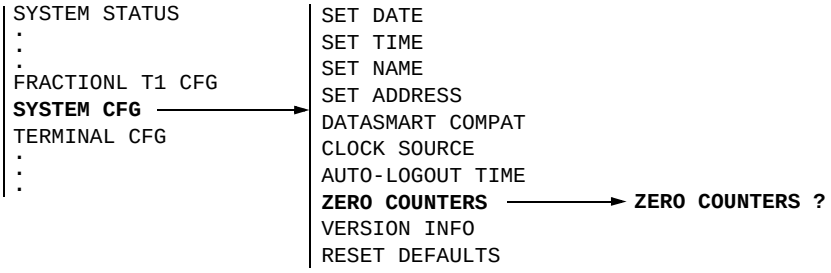
- Carrier NI Short and Long Performance reports
- Alarm History report
- Security History report

Using the command line

To zero the counters, use the **ZALL** command. You must have super-user or configuration privileges.

Using the front panel

To zero the counters from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until SYSTEM CFG appears in the display.
3. Push Select. SET DATE appears in the display.
4. Push Next or Previous until ZERO COUNTERS appears in the display.
5. Push Select. ZERO COUNTERS? appears in the display.
6. Push Select again to zero the counters, or push Escape to abort. If you push Select, the message PERF DATA CLEARD is displayed, indicating that the counters have been zeroed.

Obtaining new system software

The process for obtaining the latest DataSMART system software has three parts:

- Your company's network administrator or system administrator downloads the file from http://www.kentrox.com/support.
- The administrator then places the file on your company's TFTP host system. (The file must be in the TFTP host's default TFTP directory.) The administrator then informs you of the TFTP host's IP address.

  The TFTP IP address must be in your unit's Source Address Screening list if Source Address Screening is enabled. (See "Setting up IP source address screening" on page 184.)
- Using any active IP connection, you download new system software into the DataSMART unit's flash memory. (See Chapter 8 for information on selecting an IP connection.) After the file is successfully downloaded, enter the **BOOT:I** command to restart the unit and execute the software you just downloaded.

NOTE

Once you have booted your unit from the updated software, that software version becomes the active software version and is booted by default when you restart the unit or reset defaults. The unit stores the previous software version in what is now the inactive memory bank. To boot the previous software, enter ***BOOT:I*** *again.*

You cannot download software or boot the unit from the front panel.

Use the following command to download a software update. You must have super-user privileges.

TSWDL:*i*

i	Enter the IP address of the TFTP host where the software update is stored. Valid addresses are 0.0.0.0 to 255.255.255.255.

Use the following command to boot your DataSMART unit from either the active or inactive memory bank.

NOTE

Booting the unit will log out all users, execute the self-test, zero counters in the performance reports and clear the Carrier NI, Security History and Alarm History reports, and reset all performance data.

To boot the unit, you must have super-user privileges.

BOOT:*b*

b	Enter **I** for inactive software version or **A** (default) for currently active software version. Entering **BOOT:I** causes the inactive software version to become the active version and vice versa.

Obtaining product version information

If you call Kentrox Customer Support, you should have the model and serial numbers for your DataSMART available to give to your representative. You can obtain this information from the command line or the front panel.

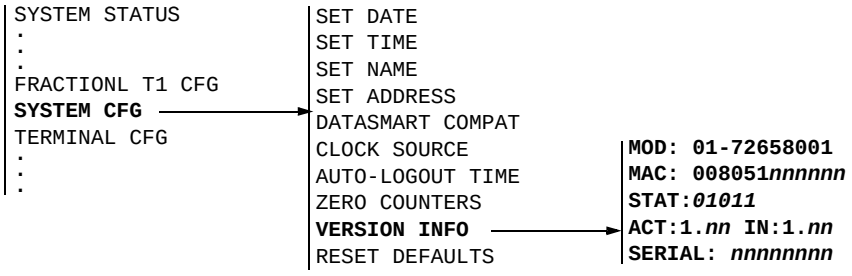
Using the command line

Use the **WYV** command to obtain version information. You need super-user, configuration, or maintenance privileges. The DataSMART displays the version information on the screen, similar to the following.

```
KENTROX      01-72658001, SERIAL nnnnnnnn,
STAT 01011, ACTIVE 1.nn, INACTIVE 1.nn
MAC ADDRESS 008051nnnnnn
```

Using the front panel

To obtain version information from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until SYSTEM CFG appears in the display.
3. Push Select. SET DATE appears in the display.
4. Push Next or Previous until VERSION INFO appears in the display.
5. Push Select, then push Next or Previous to cycle through the version information.

Resetting to default values

You can reset the DataSMART to its default power-up state at any time. The DataSMART will:

- Log out all users
- Restart its control program and execute self test
- Reset all configuration parameters to their default state, including bandwidth assignments and IP addresses
- Zero counters in the performance reports and clear the Carrier NI, Security History and Alarm History reports

Once self-test has been completed, you can log into the unit.

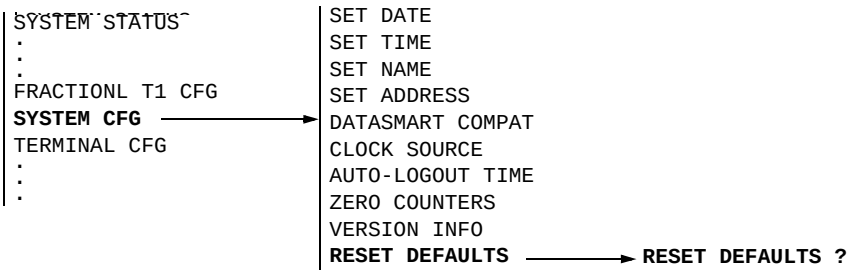
CAUTION!
A reset to defaults causes a service disruption until the DataSMART unit is reconfigured for service. (If your required configuration is identical to the default, the service disruption lasts only as long as it takes for the unit to reboot.)

Using the command line

To reset the DataSMART to its default configuration, use the **RSD** command. You must have super-user or configuration privileges.

Using the front panel

To reset defaults from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until SYSTEM CFG appears in the display.
3. Push Select. SET DATE appears in the display.
4. Push Next or Previous until RESET DEFAULTS appears in the display.
5. Push Select. RESET DEFAULTS? appears in the display. Push Select, or push Escape to abort.

Clearing stored information

The actions that cause the DataSMART to clear its configuration and performance data are summarized in Table 4.

Table 4—Actions that clear stored information from the DataSMART

Action	Clears all configuration data	Clears Carrier NI, Alarm History, and Security History reports	Clears all other reports
Set date or time (**SD** or **ST**, page 38)	Not cleared	Not cleared	Cleared
Zero all counters (**ZALL**, page 49)	Not cleared	Not cleared	Cleared
Cycle power to unit	Not cleared	Cleared	Cleared
Boot unit (**BOOT**, page 50)	Not cleared	Cleared	Cleared
Reset to defaults (**RSD**, page 52)	Cleared	Cleared	Cleared

Configuring the control port

You need to set up the control port parameters if you plan to communicate with the DataSMART via a DCE or DTE control port. These parameters must be set up regardless of whether you plan to communicate through a terminal with an ASCII connection, a modem, or a SLIP or PPP connection for Telnet or SNMP.

There are five steps to using a control port:

1. Make the physical cable connection between the port and the control device.

   Step 1 is covered thoroughly in the *DataSMART 600 Series Installation Guide*. This section does not repeat that information.

2. Establish the character protocol for the connection, including baud rate, parity, data bits, and stop bits.

3. Specify whether or not you want characters received at the control port to be echoed back to the control device.

4. Specify which control port you are using, either DCE or DTE.

   Steps 2, 3, and 4 are covered in this section.

5. Specify your serial IP network protocol (SLIP or PPP) if you are using a serial protocol for Telnet or SNMP.

   Step 5 is covered in Chapter 8, under "Selecting the IP network interface from the front panel" on page 177.

NOTE
When the unit is configured for SLIP or PPP, only IP packets are recognized on the control port. Therefore, you should set up your IP configuration as described in Chapter 7 before selecting SLIP or PPP.

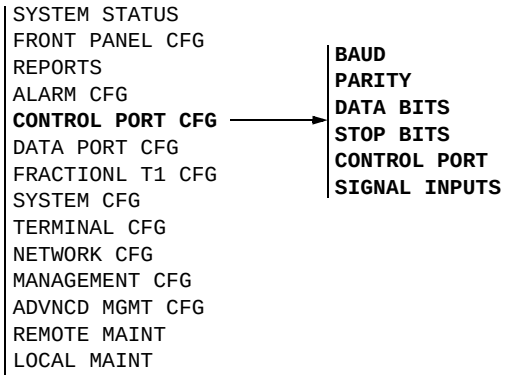
Command-line access

The commands for configuring control ports are listed below (enter **CC** to see this display).

```
                CONTROL PORT CONFIGURATION MENU
EE / DE - Enable/Disable Character Echo
DCE/DTE - Select the Control Port
CCV     - View Control Port Configuration
```

Front-panel access

The front-panel commands for configuring the control port are as follows.



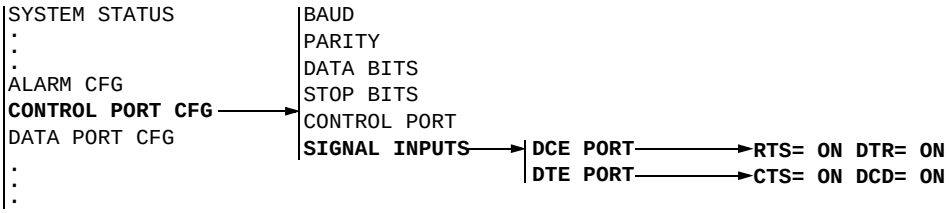
Viewing the current configuration

You can look at the current control port settings by executing the **CCV** command. This command displays the View Control Port Configuration screen, as shown below.

```
        VIEW CONTROL PORT CONFIGURATION

Echo      Control Port  Daisy Chain  CP Setup
--------  ------------  -----------  ---------
ENABLED   DCE           ENABLED       96,N,8,1

DCE Inputs  DTE Inputs
----------  ----------
RTS    DTR  CTS    DCD
---    ---  ---    ---
ON     ON   OFF    OFF
```

Field	Description
Echo	This field tells you if character echo is enabled or disabled.
Control Port	This field tells you the port at which the DataSMART receives commands and outputs alarm messages.
Daisy Chain	This field tells you if daisy-chaining is enabled or disabled.
CP Setup	This field tells you the protocol settings of the control port: baud rate in hundreds, parity, data-bits-per-character, and stop-bits-per-character.
DCE Inputs	These fields tell you the control port input signal state for RTS and DTR. Possible values for each include ON or OFF.
DTE Inputs	These fields tell you the control port input signal state for CTS and DCD. Possible values for each include ON or OFF.

Using the front panel to view DCE or DTE inputs



TIP
Both input signals must be on before you can communicate through the selected control port.

1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until CONTROL PORT CFG appears in the display.
3. Push Select. BAUD appears in the display.
4. Push Next or Previous until SIGNAL INPUTS appears in the display.
5. Push Select. DCE PORT appears in the display.
6. Push Next or Previous if you want to change to the DTE port.
7. Push Select to view the current input states for the port.

Configuring the physical connection

By default, the DataSMART is set up with the following character protocol:

baud = 9600
parity = NONE
data bits per character = 8
stop bits per character = 1

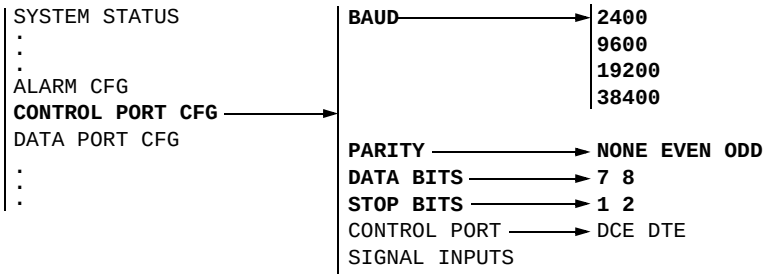
If the control device you are using is set differently from the DataSMART, you can change the settings on the control device, or you can change the settings in the DataSMART.

All settings apply to both control ports: DCE and DTE.

You cannot change the protocol settings via the command line.

Using the front panel

To change the protocol settings from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until CONTROL PORT CFG appears in the display.
3. Push Select. BAUD appears in the display.
4. Push Select if you want to change the baud rate. The current baud rate setting appears in the display.
5. Push Next or Previous to cycle through the baud rate choices: 2400, 9600, 19200, or 38400. When the rate you want is displayed, push Select.
6. Repeat steps 4 and 5 for PARITY, DATA BITS, and STOP BITS. Note that in step 5 the selected rate will be blinking.

   Allowed parity settings are: NONE, EVEN, or ODD

   Allowed data bits per character: 7 or 8

   Allowed stop bits per character: 1 or 2

Enabling/disabling character echo

When character echo is enabled, all printable characters sent to the control port are echoed back to the control device (e.g., characters are echoed on the screen of the control device). If character echo is disabled, characters are not echoed back to the control device.

The default for character echo is “enabled”.

The state of character echo is stored in the permanent nonvolatile configuration database.

Using the command line

You can use the **EE** and **DE** commands to enable or disable character echo. You must have super-user or configuration privileges.

EE	Enable character echo.
DE	Disable character echo.

You cannot enable or disable character echo from the front panel.

Specifying the control port

When you specify either DCE or DTE, you are telling the DataSMART which physical control port to use. The DataSMART will expect to receive commands via that port and will output all alarm messages or SNMP traps to that port.

If you are communicating with the DataSMART by modem, the modem will be connected to the DTE control port. In this case, use the commands described below to set the control port to DTE. In all other cases, the control device will be connected to the DCE port and you should leave the control port set to DCE.

If you are using a modem with daisy-chained DataSMART units, you must program each device in the daisy chain to use the DTE control port.

The control port setting does not take effect until you have logged out, then logged back into the DataSMART.

The default control port is DCE.

The control port setting is stored in the permanent nonvolatile configuration database.

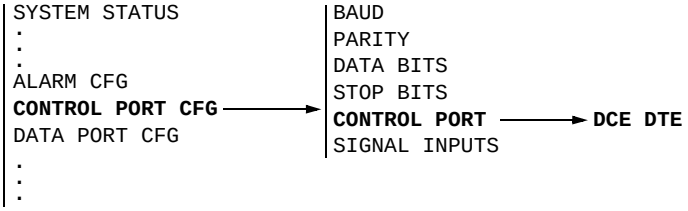
Using the command line

To specify the control port, use the **DCE** or **DTE** command. You must have super-user or configuration privileges.

DCE	Use this if any device other than a modem is connected to the control port.
DTE	Use this if a modem is connected to the control port.

Using the front panel

To specify the control port from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until CONTROL PORT CFG appears in the display.
3. Push Select. BAUD appears in the display.
4. Push Next or Previous until CONTROL PORT appears in the display.
5. Push Select. DCE DTE appears in the display. The current control port is blinking.
6. Push Next or Previous to change the current control port. When the desired value is blinking, push Select.

Configuring alarms

Using the commands in the Alarm Configuration Menu, you can configure the DataSMART to enable or disable alarm messages, set thresholds and threshold evaluation times, and change the alarm deactivation period.

TIP
If you are using an SNMP network management tool, you can enable or disable four types of SNMP traps (start, link, authentication, and enterprise) independently of whether you enable or disable alarms in ASCII. You will need to make sure your IP network interface is properly configured so that traps are sent to the right destination (see "Selecting the IP network interface from the front panel" on page 177).

As part of the overall system setup, you can specify the types of alarm messages output by the DataSMART. You can:

- Enable or disable the generation of alarm messages.
- Set the errored second (ES) and unavailable second (UAS) thresholds upon which EER alarms are generated.
- Specify the "sliding" time period for ES or UAS threshold evaluation.
- Specify whether or not an alarm should be generated on an incoming yellow condition.
- Specify the duration of the DataSMART alarm deactivation period.

Alarms are always issued in ASCII format.

This section describes how to set up the configuration parameters for alarms. If you enable alarms, you may also need to specify which control port you are using (the DCE or the DTE port), so that alarms are output correctly. By default, the alarms are output to DCE.

Command-line access

The commands for configuring alarms are listed below (enter **AC** to see this display).

```
                ALARM CONFIGURATION MENU

EAM / DAM       - Enable/Disable Alarm Messages

EYL / DYL       - Enable/Disable YELLOW Activating an Alarm
DACT:<n>        - Alarm Deactivation time in seconds, n = 1..15
EST:<n>         - Errored Second Threshold, n = 0 .. 900
UST:<n>         - Unavailable Second Threshold, n = 0 .. 900
ST15/ ST60      - Set Threshold Timing to 15 or 60 Minutes

ACV             - View Alarm Configuration
```

Front-panel access

The front-panel commands for configuring alarms are as follows.

```
SYSTEM STATUS              ALARM MESSAGES
FRONT PANEL CFG            YEL ACTIVATE ALM
REPORTS                    ALARM DEACT TIME
ALARM CFG  ------------->  ES THRESHOLD
CONTROL PORT CFG           UAS THRESHOLD
DATA PORT CFG              THRESHOLD TIMING
FRACTIONL T1 CFG
SYSTEM CFG
TERMINAL CFG
NETWORK CFG
MANAGEMENT CFG
ADVNCD MGMT CFG
REMOTE MAINT
LOCAL MAINT
```

Viewing the current configuration

Before changing the alarm configuration parameters, you may want to look at the current settings. You can do this by executing the **ACV** command. This command displays the View Alarm Configuration screen, as shown below.

```
        VIEW ALARM CONFIGURATION

Message     Alarms Activated  Alarm Deactivation
            LOS+AIS+OOF       Seconds
----------  ----------------  ------------------
DISABLED    +YEL+EER          15

EST  UST  Threshold
          Timing
---  ---  ---------
13   10   15
```

Field	Description
Message	This field tells you if alarm messages are enabled or disabled. Alarm messages, when enabled, are displayed in user (ASCII) format.
Alarms Activated	This field tells you what types of conditions generate alarms. LOS, AIS, and OOF always generate alarms; you can enable or disable alarms for EER and incoming yellow.
Alarm Deactivation Seconds	This field tells you how many seconds the DataSMART continues in an alarm state once the alarm condition has been cleared.
EST, UST	These fields tell you the alarm thresholds for errored second (ES) and unavailable second (UAS), respectively. A zero (0) value means that EER alarms for ES or UAS have been disabled.
Threshold Timing	This field tells you the “sliding” time period the DataSMART uses for ES and UAS threshold evaluation. The period can be either 15 or 60 minutes.

Enabling/disabling alarm messages

The DataSMART outputs an alarm message to your control device when it enters an alarm state. This message identifies the alarm type, the time and date of the alarm occurrence, and the device name and address of the unit sending the message.

You can disable this alarm message output. For example, you may want to do this if you are using a “polling” program to monitor alarms on the devices in your network.

The default for alarm message output is “disabled”.

NOTE

Disabling alarm messages does not affect the other alarm reporting mechanisms in the DataSMART, including the Alarm History report, the System Status report, SNMP traps, and LED illumination.

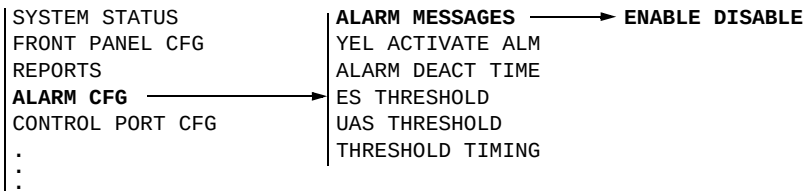
Using the command line

To enable or disable alarm messages from the command line, use the **EAM** and **DAM** commands. You need super-user or configuration privileges.

EAM	Enable alarm messages.
DAM	Disable alarm messages.

Using the front panel

To enable or disable alarm messages from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until ALARM CFG appears in the display.
3. Push Select. ALARM MESSAGES appears in the display.
4. Push Select. ENABLE DISABLE appears in the display with the current selection blinking.
5. Push Next or Previous to change the selection. When the desired choice is blinking, push Select.

Enabling/disabling alarms on incoming yellow

The DataSMART generates an alarm message if it detects an incoming yellow alarm code at the network interface, and thus notifies you of a far-end problem. If you do not want this notification, you can deactivate this alarm message. You might also want to deactivate this alarm message if you are using SF framing and are receiving bit patterns that generate a false yellow indication.

The default is to generate an alarm message on incoming yellow (enabled).

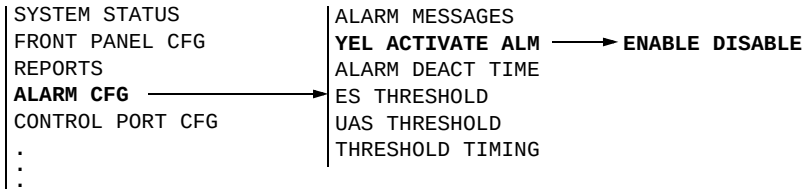
Using the command line

To enable or disable activation of an alarm on incoming yellow, use the **EYL** and **DYL** commands. You must have super-user or configuration privileges.

EYL	Enable alarm activation on incoming yellow.
DYL	Disable alarm activation on incoming yellow.

Using the front panel

To enable or disable alarm activation on an incoming yellow alarm, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until ALARM CFG appears in the display.
3. Push Select. ALARM MESSAGES appears in the display.
4. Push Next or Previous until YEL ACTIVATE ALM appears in the display.
5. Push Select. ENABLE DISABLE appears in the display with the current selection blinking.
6. Push Next or Previous to change the selection. When the desired choice is blinking, push Select.

Setting the threshold for errored seconds (ES)

You can specify that the DataSMART generate an EER alarm on excessive errored seconds (ESs). This allows you to monitor the line for errors and detect problems that are not described by signal loss or out-of-frame alarms.

You set up an EER alarm on excessive ESs by using the **EST** command to specify the error threshold. You can specify a threshold value of from 0 to 900, inclusive. A value of 0 disables EER alarm activation on errored seconds; a value of 900 means that an alarm will be generated if an ES occurs every second of a 15-minute time window (60 x 15).

You can set the time window to 15 minutes or 60 minutes by using the **ST15** or **ST60** command, respectively (see page 66). The window is a "sliding" window.

The default threshold is 13 errored seconds and the default window is 15 minutes ($\sim 10^{-8}$).

Using the command line

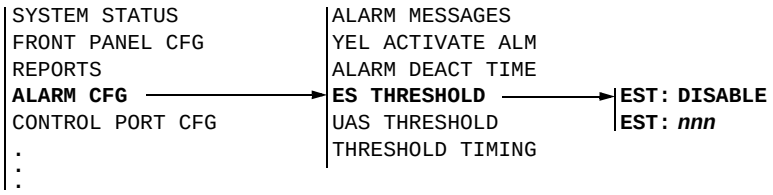
To set the ES threshold, use the **EST** command. You need super-user or configuration privileges. The command syntax is:

EST:*n*

n	Enter the number of ESs that must occur within the time window in order to activate an EER alarm. The allowed values are 0 to 900, inclusive. 0 disables EER alarm activation on an ES condition.

Using the front panel

To set the ES threshold from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until ALARM CFG appears in the display.
3. Push Select. ALARM MESSAGES appears in the display.
4. Push Next or Previous until ES THRESHOLD appears in the display.
5. Push Select. The current threshold value appears in the display: 1 ... 900, or DISABLE (off).
6. Push Next or Previous to change to the desired value, then push Select.

Setting the threshold for unavailable seconds (UAS)

If your line is experiencing chronically high error rates, you may elect to disable the errored second (ES) threshold and just use the unavailable second (UAS) threshold for generating EER alarms. This decreases the alarm sensitivity significantly, since a UAS occurs at the onset of ten consecutive severely errored seconds (SESs).

You use the **UST** command to specify the threshold used for generating an EER alarm on UASs. You can specify a threshold value of from 0 to 900, inclusive. A value of 0 disables EER alarm activation on unavailable seconds; a value of 900 means that an EER alarm will be generated if an unavailable second occurs every second of a 15-minute time window (60 x 15).

You can set the time window to 15 minutes or 60 minutes by using the **ST15** or **ST60** command, respectively (see page 66). The window is a "sliding" window.

The default threshold is 10 unavailable seconds and the default time window is 15 minutes.

Using the command line

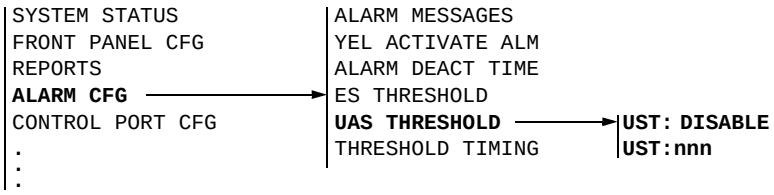
To set the UAS threshold, use the **UST** command. You need super-user or configuration privileges. The syntax for the command is:

UST:*n*

n	Enter the number of UASs that must occur within the time window in order to activate an EER alarm. The allowed values are 0 to 900, inclusive. 0 disables alarm activation on a UAS condition.

Using the front panel

To set the UAS threshold from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until ALARM CFG appears in the display.
3. Push Select. ALARM MESSAGES appears in the display.
4. Push Next or Previous until UAS THRESHOLD appears in the display.
5. Push Select. The current threshold setting appears in the display.
6. Push Next or Previous to change to the desired value, then push Select.

Specifying the error threshold evaluation window

You can a specify a 15-minute or a 60-minute "sliding" time window for error threshold evaluation. If the specified error threshold is exceeded during this sliding window, the DataSMART generates an EER alarm. Use the 15-minute window for increased error sensitivity; use the 60-minute window for a longer term view of line quality.

The following table relates evenly distributed bit error rates and the number of ESs that will occur in 15- and 60-minute time periods.

Error rate	ESs in 15 minutes	ESs in 60 minutes
1×10^{-6}	900	—
1×10^{-7}	135	540
1×10^{-8}	13	54
1×10^{-9}	1	5

The default window for threshold evaluation is 15 minutes.

Using the command line

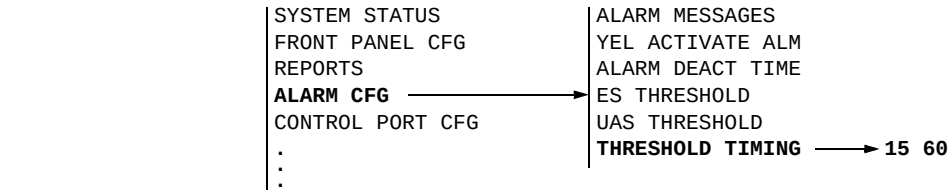
To specify the sliding window for threshold evaluation, use the **ST15** and **ST60** commands. You must have super-user or configuration privileges.

ST15 Set the sliding window to 15 minutes.

ST60 Set the sliding window to 60 minutes.

Using the front panel

To set the sliding window from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until ALARM CFG appears in the display.
3. Push Select. ALARM MESSAGES appears in the display.
4. Push Next or Previous until THRESHOLD TIMING appears in the display.
5. Push Select. 15 60 appears in the display. The current value is blinking.
6. Push Next or Previous to change the value, then push Select.

Setting the alarm deactivation time

You can program the DataSMART to remain in an alarm state up to 15 seconds after an alarm condition has cleared. This deactivation period applies to the following alarms:

- NI LOS and TI LOS
- NI AIS and TI AIS
- NI OOF and TI OOF
- NI YEL and TI YEL
- NI EER and TI EER

It does not apply to:

- ECF

The default alarm deactivation time is 15 seconds.

Using the command line

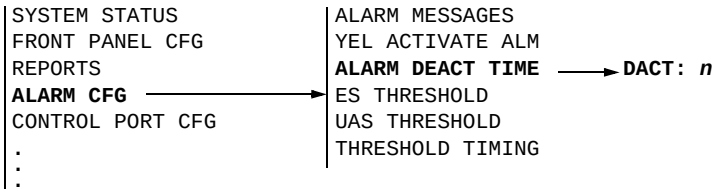
To set the alarm deactivation time, use the **DACT** command. You must have super-user or configuration privileges. The command syntax is:

DACT:*n*

n Set the deactivation time from 1 to 15 seconds.

Using the front panel

To set the alarm deactivation time from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until ALARM CFG appears in the display.
3. Push Select. ALARM MESSAGES appears in the display.
4. Push Next or Previous until ALARM DEACT TIME appears in the display.
5. Push Select. The current alarm deactivation period appears in the display: 1 ... 15 seconds.
6. Push Next or Previous to change the value, then push Select.

CHAPTER

5 Configuring interfaces

This chapter covers the following topics:

- Configuring the network interface
- Configuring the terminal interface (add/drop units only)
- Configuring the data port
- Assigning network interface channels to the data port

Configuring the network interface

Configure the network interface so that it is compatible with the T1 signal from the service provider. A properly configured network interface provides the requested performance reports, remote loopbacks and alarms; and, optionally, it establishes a data link path for managing a far-end unit.

The DataSMART network interface should be configured for compatibility with the T1 signal received from the service provider.

You must set up the network interface parameters to match the requirements of your service provider. The framing format and line coding for the DataSMART must match the framing format and line coding of your T1 line. Further, the line build-out should always be left at 0.0 dB unless another value is specifically requested. Increased attenuation can interfere with the T1 service.

All these commands apply to both the transmit and receive directions on the network interface. There is no way to configure the two directions separately.

Command-line access

The commands for configuring the network interface parameters are listed below. To view this menu, log into the unit you want to configure, then enter **NC**.

DataSMART 658 only

```
          NI CONFIGURATION MENU

NSF/NESF/NERC     - NI SF/ESF/Ericsson Framing Format
NAMI / NB8        - NI AMI/B8ZS Line Coding
EPRM / DPRM       - Enable/Disable T1.403 PRM Generation out NI
FKA / UKA         - Framed/Unframed Keep Alive
EYEL / DYEL       - Enable/Disable YELLOW Activation out NI
ADR54:<Trgt>      - 54016 Address = C(CSU), D(DSU), or B(Both)
E54 / D54         - Enable/Disable 54016 Mode

                Line Build Out
NL0                -  0.0 dB
NL1                -  7.5 dB
NL2                - 15.0 dB

NCV                - View NI Configuration
```

Front-panel access

The front-panel commands for configuring the network interface are as follows.

```
SYSTEM STATUS
FRONT PANEL CFG
REPORTS
ALARM CFG
CONTROL PORT CFG
DATA PORT CFG
FRACTIONL T1 CFG
SYSTEM CFG
TERMINAL CFG
NETWORK CFG ──────────►  FRAMING FORMAT
MANAGEMENT CFG           LINE CODING
ADVNCD MGMT CFG          54016 ADDRESS
REMOTE MAINT             54016 MODE
LOCAL MAINT              PRM GENERATION
                         YEL GENERATION
                         KEEP ALIVE
                         LINE BUILD OUT
```

You can use the View Network Configuration display to see the current network interface settings. Enter **NCV** at the command-line prompt.

```
        VIEW NETWORK CONFIGURATION

Framing  Line Code  Line Build Out  PRM Generation  Keep Alive
-------  ---------  --------------  --------------  ----------
ESF      B8ZS       0.0 dB          DISABLED        FRAMED 1íS

YEL Generation  54016 Address  54016 Mode
--------------  -------------  ----------
ENABLED         EITHER         DISABLED
```

Field	Description
Framing	This displays the current network framing: SF (super frame), ESF (extended super frame), or ERICS (Ericsson-modified super frame).
Line Code	This displays the current line coding: AMI or B8ZS.
Line Build Out	This displays the state of line build-out at the network interface. Possible values are 0.0 dB, 7.5 dB, or 15.0 dB.
PRM Generation	This displays the state of ANSI T1.403 Performance Report Message (PRM) generation: ENABLED or DISABLED.
Keep Alive	This displays the state of the Framed Keep Alive option: FRAMED 1s or AIS. It is valid only for add/drop units with all DS0 channels assigned to the terminal interface.
YEL Generation	This displays the state of yellow alarm generation at the network interface: ENABLED or DISABLED. It is valid only for add/drop units with all DS0 channels assigned to the terminal interface.
54016 Address	This displays the currently selected 54016 address filter: DSU, CSU, or EITHER.
54016 Mode	This displays the state of 54016 transmission: ENABLED or DISABLED.

Specifying NI framing format

TIP
*The following framing formats and line codes usually go together: super frame and AMI (**NSF** and **NAMI**); and extended super frame and B8ZS (**NESF** and **NB8**). However, one does not depend on the other.*

You must set the DataSMART network interface to recognize and transmit data in the same framing format used by the incoming T1 line. Three format choices are available: super frame (SF), extended super frame (ESF), or Ericsson-modified super frame.

Note that if the incoming T1 line is in SF format, you may want to disable the DataSMART from generating alarms upon detection of incoming yellow at the network interface. Sometimes data patterns in SF format generate false yellow. See "Enabling/disabling alarms on incoming yellow" on page 63.

Also, the option of using the facility data link (FDL) for the Data Link path is available only if the NI framing format is set to extended super frame (ESF). See "Selecting an IP network interface from the command line" on page 176.

The default framing format is extended super frame (ESF).

Using the command line

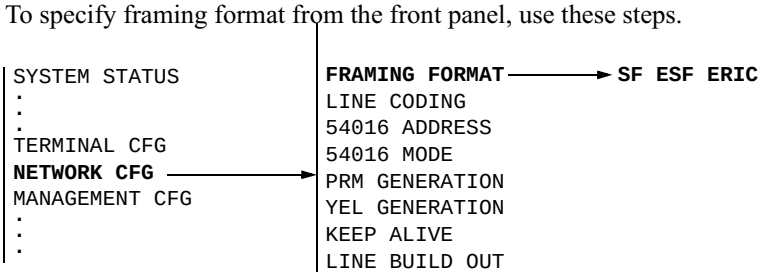
Use the following commands to specify framing format. You must have super-user or configuration privileges.

NSF	Super frame
NESF	Extended super frame
NERC	Ericsson-modified super frame

NOTE
Framing format "NERC" is the framing format used by some L. M. Ericsson switches in wireless service.

Using the front panel

To specify framing format from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until NETWORK CFG appears in the display.
3. Push Select. FRAMING FORMAT appears in the display.
4. Push Select. SF ESF ERIC appears in the display. The currently selected format is blinking.
5. Push Next or Previous until the format you want is blinking, then push Select.

Specifying NI line coding

You must set the DataSMART network interface to the line coding specified by your service provider. Two selections are available: AMI (alternate mark inversion) or B8ZS (binary 8 zeroes substitution).

The default line coding is B8ZS.

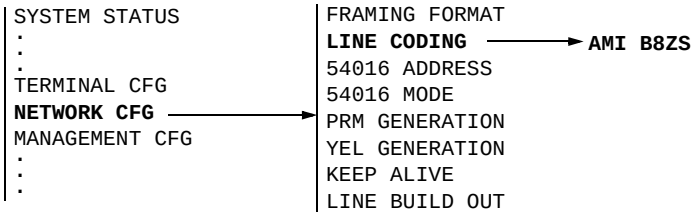
Using the command line

Use the following commands to specify line coding. You must have super-user or configuration privileges.

NAMI	AMI line coding
NB8	B8ZS line coding

Using the front panel

To specify line coding from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until NETWORK CFG appears in the display.
3. Push Select. FRAMING FORMAT appears in the display.
4. Push Next or Previous until LINE CODING appears in the display.
5. Push Select. AMI B8ZS appears in the display. The currently selected value is blinking.
6. Push Next or Previous until the line coding you want is blinking, then push Select.

Enabling/disabling T1.403 loopback and PRM generation

You can enable or disable the DataSMART from sending and receiving ANSI T1.403 performance report messages (PRMs). You should enable T1.403 PRMs if either of the following is true:

- Your carrier requires T1.403 PRMs
- You have a point-to-point application and you want to get far-end performance reports at the near end

When T1.403 mode is enabled, the DataSMART does the following:

- Sends PRMs out the network interface to the far-end device
- Receives PRMs from the far-end device (used to collect data for far-end reports)
- Sets and resets remote loopbacks using T1.403-standard codes

When T1.403 mode is enabled, the DataSMART defaults to T1.403 standards for setting and resetting loopbacks, even if 54016 mode is enabled.

The default state is T1.403 mode disabled.

Using the command line

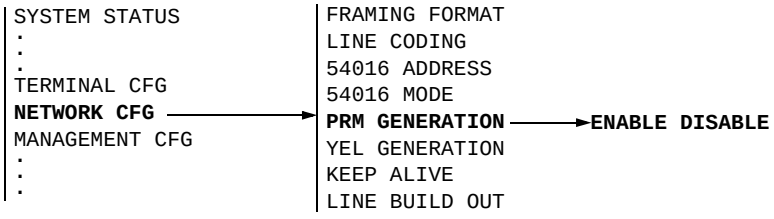
Use the following commands to enable or disable T1.403 mode. You must have super-user or configuration privileges.

EPRM Enable sending and receiving ANSI T1.403 PRMs and loopback set and reset codes.

DPRM Disable sending PRM messages to the network and disable all other activities defined by the standard.

Using the front panel

To enable or disable T1.403 mode from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until NETWORK CFG appears in the display.
3. Push Select. FRAMING FORMAT appears in the display.
4. Push Next or Previous until PRM GENERATION appears in the display.
5. Push Select. ENABLE DISABLE appears in the display. The currently configured value is blinking.
6. Push Next or Previous until the setting you want is blinking, then push Select.

Selecting the 54016 address

If the network framing format is ESF and 54016 mode is enabled, you can specify whether the DataSMART responds to 54016 requests addressed to a DSU, a CSU, or both. (See the next entry for procedures on enabling 54016 mode.)

The default is for the DataSMART to respond to both CSU and DSU requests. If you want the DataSMART to respond only to DSU or CSU requests, set the 54016 mode appropriately.

Using the command line

Use the following command to specify the 54016 address mode. You must have super-user or configuration privileges. The command syntax is:

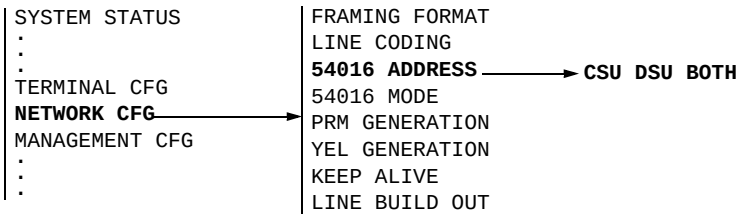
ADR54:*Trgt*

where *Trgt* is:

D	DSU
C	CSU
B	both DSU and CSU

Using the front panel

To specify the 54016 address mode from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until NETWORK CFG appears in the display.
3. Push Select. FRAMING FORMAT appears in the display.
4. Push Next or Previous until 54016 ADDRESS appears in the display.
5. Push Select. CSU DSU BOTH appears in the display. The currently configured value is blinking.
6. Push Next or Previous until the setting you want is blinking, then push Select.

Enabling/disabling 54016 mode

You can enable or disable the DataSMART from responding to requests that comply with the message format of AT&T TR54016, Issue 2. When enabled for 54016, the DataSMART can do the following:

- Respond to 54016 requests
- Set and reset remote loopbacks using 54016 requests, if T1.403 is disabled (see "Enabling/disabling T1.403 loopback and PRM generation" on page 74)

The network interface must be set to ESF format (see "Specifying NI framing format" on page 72) before you enable 54016 mode. This is because 54016 requests are received and sent via the ESF facility data link.

The default is 54016 mode disabled.

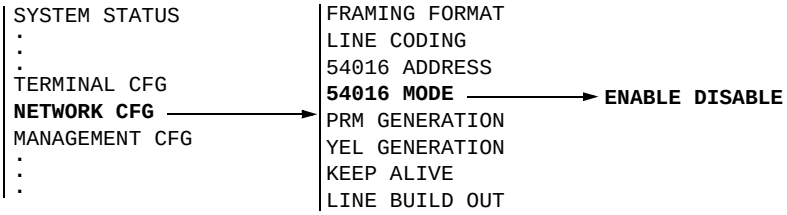
Using the command line

Use these commands to enable or disable 54016 mode. You must have super-user or configuration privileges.

E54	Enable 54016 mode.
D54	Disable 54016 mode.

Using the front panel

To enable or disable 54016 mode from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until NETWORK CFG appears in the display.
3. Push Select. FRAMING FORMAT appears in the display.
4. Push Next or Previous until 54016 MODE appears in the display.
5. Push Select. ENABLE DISABLE appears in the display. The currently configured value is blinking.
6. Push Next or Previous until the setting you want is blinking, then push Select.

Enabling/disabling yellow alarm output (add/drop units only)

This command has no effect unless all channels are assigned to the terminal interface.

Yellow alarm output should be enabled only if the terminal equipment connected to the DataSMART is incapable of generating a yellow alarm.

If yellow alarm output is enabled, the DataSMART generates and transmits the yellow alarm code toward the network any time an alarm condition is detected on the network interface. The yellow alarm is transmitted two to three seconds after alarm conditions AIS, OOF or LOS arise.

If the alarm output is disabled, the DataSMART will not generate a yellow alarm code.

The default for alarm generation on incoming yellow is disabled.

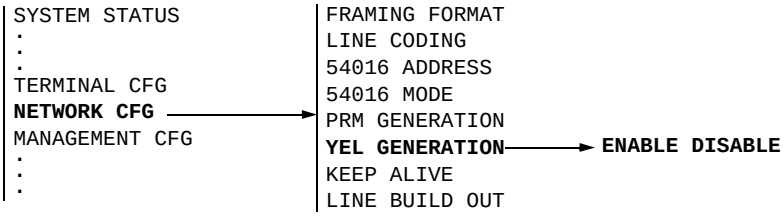
Using the command line

Use the following commands to enable or disable yellow alarm generation. You must have super-user or configuration privileges.

EYEL	Enable generation of yellow alarm.
DYEL	Disable generation of yellow alarm.

Using the front panel

To specify a framed or unframed keep-alive signal from the front panel, use these steps.



Push Escape until SYSTEM STATUS appears in the display.

1. Push Next or Previous until NETWORK CFG appears in the display.
2. Push Select. FRAMING FORMAT appears in the display.
3. Push Next or Previous until YEL GENERATION appears in the display.
4. Push Select. ENABLE DISABLE appears in the display. The currently configured value is blinking.
5. Push Next or Previous until the setting you want is blinking, then push Select.

Specify the “keep alive” signal for the network interface (add/drop units only)

This command has no effect unless all channels are assigned to the terminal interface.

If the terminal interface enters an out-of-frame (OOF) condition, the DataSMART keeps the network connection alive by sending the network a framed all-1s signal. This masks the presence of an alarm at the terminal end.

You can program the DataSMART to send the network an AIS alarm (unframed all-1s signal) when the terminal signal is out of frame. This generates an alarm at the far end.

The default “keep-alive” signal is a framed all-1s signal.

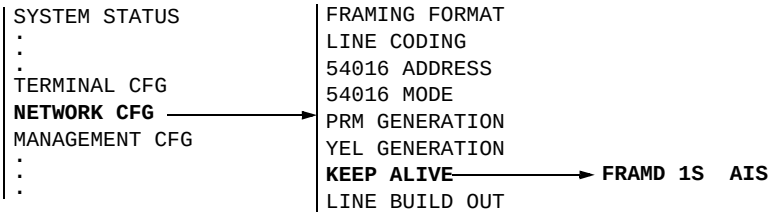
Using the command line

Use the **FKA** and **UKA** commands to specify the keep alive signal. You must have super-user or configuration privileges.

FKA	Send a framed all-1s signal.
UKA	Send AIS (unframed all-1s signal).

Using the front panel

To specify a framed or unframed keep-alive signal from the front panel, use these steps.



Push Escape until SYSTEM STATUS appears in the display.

1. Push Next or Previous until NETWORK CFG appears in the display.
2. Push Select. FRAMING FORMAT appears in the display.
3. Push Next or Previous until KEEP ALIVE appears in the display.
4. Push Select. Two values, FRAMD 1S and AIS, appear in the display. The currently configured value is blinking.
5. Push Next or Previous until the setting you want is blinking, then push Select.

Specifying transmit line build out attenuation

Your service provider may ask you to set the DataSMART to attenuate (reduce) the T1 signal at the network interface. Three line attenuation settings are available: 0.0 dB (no attenuation), 7.5 dB, or 15 dB.

The default line attenuation is 0.0 dB.

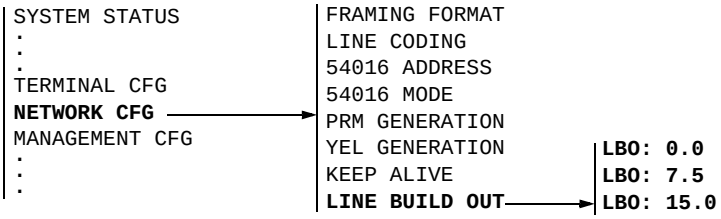
Using the command line

Use the following commands to specify line attenuation. You must have super-user or configuration privileges.

NL0	0.0 dB line attenuation
NL1	7.5 dB line attenuation
NL2	15.0 dB line attenuation

Using the front panel

To specify line attenuation from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until NETWORK CFG appears in the display.
3. Push Select. FRAMING FORMAT appears in the display.
4. Push Next or Previous until LINE BUILD OUT appears in the display.
5. Push Select. The current LBO setting appears in the display.
6. Push Next or Previous to change the LBO setting to the one you want, then push Select.

Configuring the terminal interface (add/drop units only)

Configure the unit's terminal interface so that its framing format, line coding, idle code, and signal equalization are all compatible with your terminal equipment.

You must configure the terminal interface of the DataSMART add/drop unit to make it compatible with the terminal equipment (T1 customer premise equipment) connected to it.

All these commands apply to both the transmit and receive directions on the terminal interface.

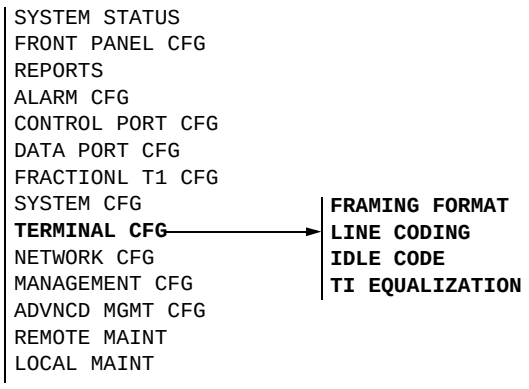
Command-line access

The commands for configuring the terminal interface parameters are listed below (enter **TC** to see this display).

```
                  TI CONFIGURATION MENU

TSF/TESF/TERC  - TI SF/ESF/Ericsson Framing Format
TAMI / TB8     - TI AMI/B8ZS TI Line Coding
TIDL:<c>       - Idle Code, c = 00-FF Hex

                  TI Equalization
TE0            -   0 - 133 ft
TE1            - 133 - 266 ft
TE2            - 266 - 399 ft
TE3            - 399 - 533 ft
TE4            - 533 - 655 ft

TCV            - View TI Configuration
```

Front-panel access

The front-panel commands for configuring the terminal interface are as follows.



Viewing the current TI configuration

Before changing any terminal interface parameters, you may want to look at the current settings. To do this, enter **TCV** at the command-line prompt. This produces a display similar to the one below.

```
       VIEW TERMINAL CONFIGURATION

Framing    Line    Equalization     Idle
Format     Code                     Code

-------    ----    ------------   ------
ESF        B8ZS    0..133 ft      7F Hex
```

Field	Description
Framing format	This displays the current framing format applied to the terminal interface: SF (super frame), ESF (extended super frame), or ERICS (Ericsson-modified super frame).
Line code	This displays the current line coding applied to the terminal interface: AMI or B8ZS.
Equalization	This displays the state of signal equalization at the terminal interface: 0..133ft, 133..266ft, 266..399ft, 399..533ft, or 533..655ft.
Idle code	This displays the currently selected idle code. The range is 00 to FF hex.

Specifying TI framing format

TIP
*The following framing formats and line codes often go together: super frame and AMI (**NSF** and **NAMI**); and extended super frame and B8ZS (**NESF** and **NB8**). However, one does not depend on the other.*

You must set the DataSMART terminal interface to recognize and transmit data in the same framing format used by the terminating customer premises equipment, usually a T1 channel bank or digital PBX. You can choose: super frame (SF; also known as D4), extended super frame (ESF), or Ericsson-modified super frame.

The default framing format is extended super frame (ESF).

Using the command line

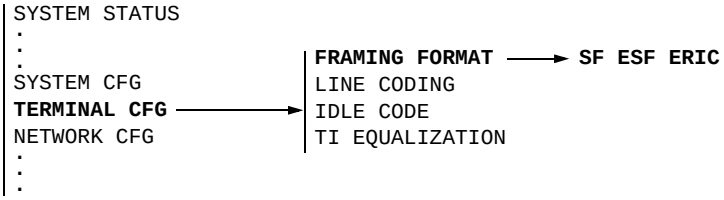
Use the following commands to set the framing format applied at the terminal interface.

TSF	Super frame
TESF	Extended super frame
TERC	Ericsson-modified super frame

NOTE
Framing format "TERC" is the framing format used by some L. M. Ericsson switches in wireless service.

Using the front panel

To specify framing format from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until TERMINAL CFG appears in the display.
3. Push Select. FRAMING FORMAT appears in the display.
4. Push Select. SF ESF ERIC appears in the display. The currently configured value is blinking.
5. Push Next or Previous until the setting you want is blinking, then push Select.

Specifying TI line coding

You must set the DataSMART terminal interface to the same line coding used by the customer premises equipment. Two selections are available: AMI (alternate mark inversion) or B8ZS (binary 8 zeroes substitution).

The default line coding is B8ZS.

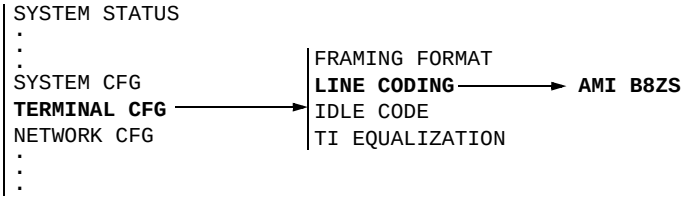
Using the command line

Use the following commands to specify line coding. You must have super-user or configuration privileges.

TAMI	AMI line coding
TB8	B8ZS line coding

Using the front panel

To specify line coding from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until TERMINAL CFG appears in the display.
3. Push Select. FRAMING FORMAT appears in the display.
4. Push Next or Previous until LINE CODING appears in the display.
5. Push Select. AMI B8ZS appears in the display. The currently configured value is blinking.
6. Push Next or Previous until the setting you want is blinking, then push Select.

Specifying TI idle code

You can specify the eight-bit idle code that is put into the unused DS0 channels of the terminal interface. The code may have any hex value between 00 and FF.

Whenever an out-of-frame condition occurs at the network interface, the DataSMART DSU puts the idle code into all channels assigned to the terminal interface.

The unit continuously transmits the idle code on any NI channel assigned to “idle”.

The default idle code is 7F hex.

Using the command line

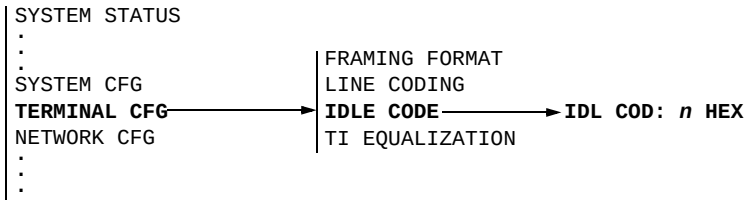
Use the **TIDL** command to specify the eight-bit idle code. You must have super-user or configuration privileges. The command syntax is:

TIDL:*c*

c Enter a hex number with a value between 00 and FF.

Using the front panel

To specify the idle code from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until TERMINAL CFG appears in the display.
3. Push Select. FRAMING FORMAT appears in the display.
4. Push Next or Previous until IDLE CODE appears in the display.
5. Push Select. The current idle code value appears in the display.
6. Push Next or Previous until the value you want appears in the display, then push Select.

Specifying TI signal equalization

If the cable between the DataSMART and the customer premises equipment is longer than 133 feet, you may need to boost the signal level being output from the terminal interface. By using the **TE***n* commands, you can specify that the terminal interface outputs a DSX-level signal equalized for cable lengths up to 655 feet.

The default equalization setting is 0.

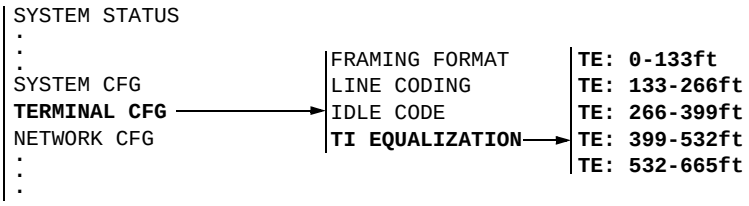
Using the command line

Use the following commands to equalize the T1 signal at the terminal interface. You must have super-user or configuration privileges.

TE0	0 - 133 feet
TE1	133 - 266 feet
TE2	266 - 399 feet
TE3	399 - 533 feet
TE4	533 - 655 feet

Using the front panel

To specify the signal equalization from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until TERMINAL CFG appears in the display.
3. Push Select. FRAMING FORMAT appears in the display.
4. Push Next or Previous until TI EQUALIZATION appears in the display.
5. Push Select. The current TI equalization configuration appears in the display.
6. Push Next or Previous until you see the equalization you want, then push Select.

Configuring the data port

You can change characteristics of the data port, including timing characteristics, idle character, and loss-of-signal indicator. Changing these parameters often requires changes at the far end or DTE as well.

You must configure the data port to match the configuration of the data terminal equipment (DTE) to which it is attached.

Most applications can use the default values. "Tail" circuits, long DTE cables at high data rates, and perhaps other situations identified by your technical support representative may require changing the settings from their default values.

Command-line access

The commands for configuring the data port are listed below. To view this menu, log into the unit you want to configure, then enter **DC**.

```
                DATA PORT CONFIGURATION MENU

EDI<n> / DDI<n> - Enable/Disable Data Inversion at Data Port, n=1
SCLK<n>:<clk>   - Source Clock at Data Port, n=1
                  clk = I (Internal), E (External)
TCLK<n>:<cmd>   - Transmit Clock Inversion at Data Port, n=1
                  cmd = E (Enable), D (Disable)
RCLK<n>:<cmd>   - Receive Clock Inversion at Data Port, n=1
                  cmd = E (Enable), D (Disable)
IDL<n>:<char>   - Idle Character at Data Port, n=1
                  char = 7E, 7F, FF
DPLOS<n>:<los>  - LOS Input Signal at Data Port, n=1
                  los = R (RTS), D (DTR), B (Both), N (No Processing)

DCV             - View Data Port Configuration
```

Front-panel access

The front-panel commands for configuring the data port are as follows.

```
SYSTEM STATUS
FRONT PANEL CFG
REPORTS
ALARM CFG                    DP DATA INVERT
CONTROL PORT CFG             DP CLK SOURCE
DATA PORT CFG  ------------> DP TX CLK INVERT
FRACTIONL T1 CFG             DP RX CLK INVERT
SYSTEM CFG                   DP IDLE CODE
TERMINAL CFG                 DP LOS INPUT SIG
NETWORK CFG
MANAGEMENT CFG
ADVNCD MGMT CFG
REMOTE MAINT
LOCAL MAINT
```

Viewing the current data port configuration

Before changing any data port parameters, you may want to look at the current settings. To do this, enter **DCV** at the command-line prompt. This produces a display similar to the one shown below.

```
        VIEW DATA PORT CONFIGURATION

                 Port 1
                --------
Data  Inversion DISABLED
Source Clock    INTERNAL
Tx Clock Invert DISABLED
Rx Clock Invert DISABLED
Idle Character  FF
LOS Input       RTS
```

Field	Description
Data Inversion	This tells you whether or not data inversion is enabled at the data port. If inversion is enabled, the data is inverted in both directions (i.e., the data from the DTE is inverted before being transmitted to the network, and vice versa).
Source Clock	This tells you which clock signal is being used to clock in transmit data at the data port: INTERNAL or EXTERNAL.
Tx Clock Invert	This tells you whether or not transmit clock inversion is enabled at the data port. If inversion is enabled, transmit data is sampled on the rising edge of the clock signal. If inversion is disabled, transmit data is sampled on the falling edge of the clock signal.
Rx Clock Invert	This tells you whether or not receive clock inversion is enabled. If inversion is enabled, receive data is changed on the falling edge of the clock signal. If inversion is disabled, receive data is changed on the rising edge of the clock signal.
Idle Character	This tells you the specified idle character for the data port: 7E, 7F, or FF hex.
LOS Input	This tells you which signals are currently being used to determine an LOS condition at the data port: RTS, DTR, BOTH, or NONE.

Enabling/disabling data inversion

These commands enable or disable data inversion at the data port. When you enable data inversion, all data received from the DTE is inverted: zeroes are changed to ones and ones are changed to zeroes before being transmitted to the network. Data received from the network is also inverted before being transmitted to the DTE. When data is inverted locally, it must also be inverted at the far-end device.

Data inversion is seldom necessary. It is sometimes used to resolve "ones density" problems caused by a high proportion of zeroes in the bit stream of the incoming or outgoing data.

The default state is data inversion disabled.

Using the command line

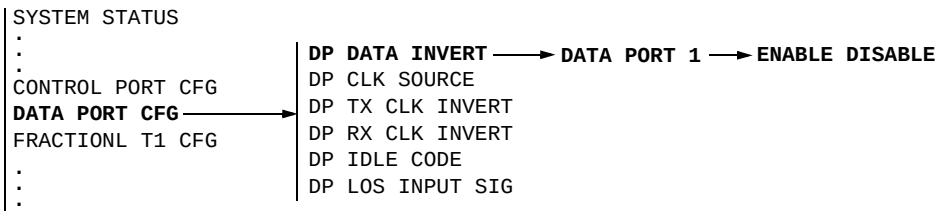
Use the following commands to enable or disable data inversion. You must have superuser or configuration privileges. The command syntax is:

EDI1 Enable data inversion at the data port.

DDI1 Disable data inversion at the data port.

Using the front panel

To specify the data port clock from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until DATA PORT CFG appears in the display.
3. Push Select. DP DATA INVERT appears in the display.
4. Push Select. DATA PORT 1 appears in the display.
5. Push Select. ENABLE DISABLE appears in the display. The currently configured value is blinking.
6. Push Next or Previous until the setting you want is blinking, then push Select.

Specifying data port clocking

You can specify the clock signal used to clock transmit (Tx) data at the data port (see Figure 5). Two clock selections are available: internal or external.

Internal clocking means that the transmit data is clocked by the data port's internal clock, which is derived from the DataSMART system source clock.

External clocking means that the transmit data is clocked by a signal received on the data port connector's external clock pins (see Table 17 on page 221).

External clocking is typically used:

- With long cables (exceeding 50-100 feet) at high data rates with DTE that supports an external clock signal
- If the DataSMART unit is driving a tail circuit (see "Specifying the system clock" on page 44)
- If the DataSMART unit is connected to a Cisco router

The normal operation of synchronous serial data ports provides for three clock signals (see Figure 5):

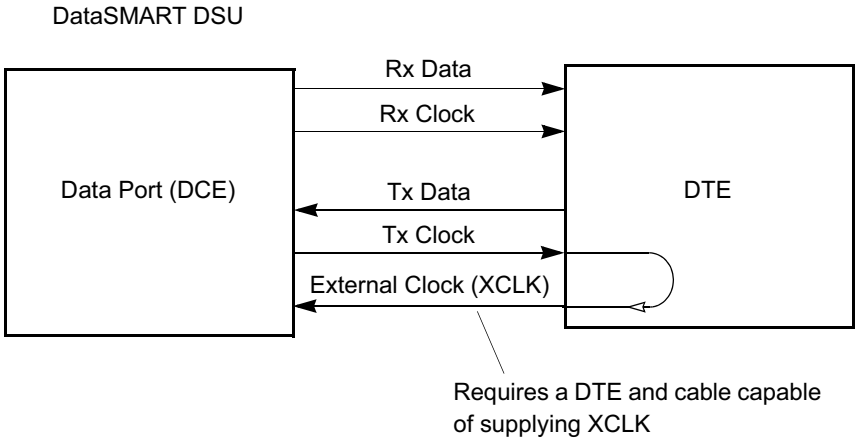
1. The DCE supplies the receive (Rx) clock signal synchronized with the receive (Rx) data.
2. The DCE also supplies the transmit (Tx) clock signal. The DTE normally transmits its data synchronized to this signal. Most data terminal equipment uses this signal.
3. The external clock signal is generated by the DTE and is used in two different applications. The first application is when you are using the external clock signal for tail circuit timing of the T1 circuit. In this application, the external clock signal is supplied by the DTE equipment. (See "Specifying the system clock" on page 44 for more information about tail circuit timing.)

   In the second application, the external clock signal is the Tx clock signal regenerated by the DTE and synchronized with the DTE's transmitted data. Usually you employ this option when you are receiving excessive data errors at the data port due to cable propagation delay. Propagation delay becomes a problem when you are using a long data cable (exceeding 50 - 100 feet) at high data rates. Propagation delay can cause significant phase shift between the Tx clock signal from the DataSMART and the Tx data signal from the DTE.

NOTE

Not all data terminal equipment supports an external clock signal. You must have terminal equipment capable of supplying this signal, however, in order to use the DataSMART plug-in's external data port clock option.

Figure 5—Clock signals at the data port



The default data port clock is internal.

TIP
***SCLK** specifies data port clocking, not system clocking. System clocking is specified with the **CLK** command.*

Using the command line

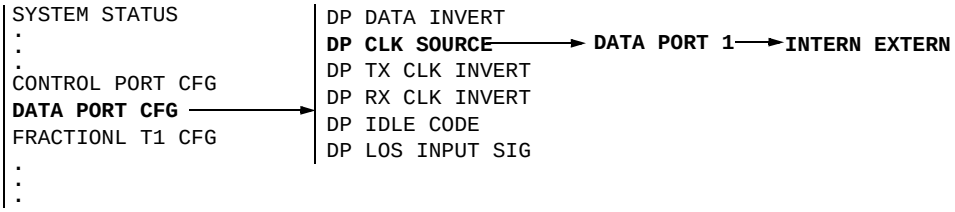
Use the **SCLK** command to specify the data port clock. You must have super-user or configuration privileges. The command syntax is:

SCLK1:*clk*

clk	Enter **E** to specify an external clock source, or enter **I** to specify the internal clock source.

Using the front panel

To specify the data port clock from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until DATA PORT CFG appears in the display.
3. Push Select. DP DATA INVERT appears in the display.
4. Push Next or Previous until DP CLK SOURCE appears in the display.
5. Push Select. DATA PORT 1 appears in the display.
6. Push Select. INTERN EXTERN appears in the display. The currently configured value is blinking.
7. Push Next or Previous until the setting you want is blinking, then push Select.

Enabling/disabling transmit clock inversion

You can invert the transmit (Tx) clock signal and, by doing so, change the clock edge being used to sample transmit (Tx) data at the data port (refer to Figure 5 on page 90). Transmit data is normally sampled on the falling edge of the transmit clock. If you invert the clock signal, data is sampled on the rising edge of the clock.

The inversion is done on the data port TCLK signal when internal source clocking is chosen and on the XCLK signal when external source clocking is chosen.

Sampling data on the falling edge of the clock is standard; you will seldom need to invert the clock. If the far-end is experiencing data errors, or if the cable connecting the DTE to the data port is long enough to cause undue propagation delays, you may need to invert the clock edge.

The default state is transmit clock inversion disabled.

Using the command line

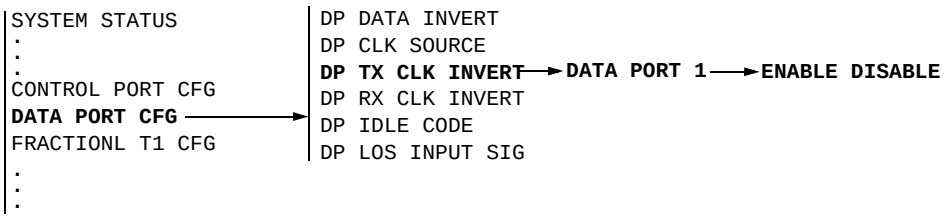
Use the **TCLK** command to invert the clock edge. You must have super-user or configuration privileges. The command syntax is:

TCLK1:*cmd*

cmd	Enter **E** to enable clock inversion, or enter **D** to disable clock inversion.

Using the front panel

To enable transmit clock inversion from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until DATA PORT CFG appears in the display.
3. Push Select. DP DATA INVERT appears in the display.
4. Push Next or Previous until DP TX CLK INVERT appears in the display.
5. Push Select. DATA PORT 1 appears in the display.
6. Push Select. ENABLE DISABLE appears in the display. The currently configured value is blinking.
7. Push Next or Previous until the setting you want is blinking, then push Select.

Enabling/disabling receive clock inversion

You can invert the receive (Rx) clock signal and, by doing so, change the clock edge being used to clock the receive (Rx) data from the data port to the DTE (refer back to Figure 5 on page 90). Normally, receive data is changed on the rising edge of the receive clock. If you invert the clock signal, receive data is changed on the falling edge of the clock.

Changing receive data on the rising edge of the clock is standard; you will seldom need to invert the clock. If the local DTE is receiving data errors, or if the cable connecting the data port and DTE is long enough to cause undue propagation delays, you may need to invert the clock edge.

The default state is receive clock inversion disabled.

Using the command line

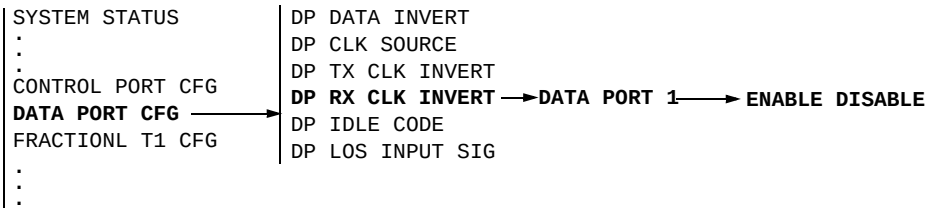
To enable or disable clock inversion, use this command:

RCLK1:*cmd*

cmd	Enter **E** to enable clock inversion, or enter **D** to disable clock inversion.

Using the front panel

To enable receive clock inversion from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until DATA PORT CFG appears in the display.
3. Push Select. DP DATA INVERT appears in the display.
4. Push Next or Previous until DP RX CLK INVERT appears in the display.
5. Push Select. DATA PORT 1 appears in the display.
6. Push Select. ENABLE DISABLE appears in the display. The currently configured value is blinking.
7. Push Next or Previous until the setting you want is blinking, then push Select.

Specifying the data port idle character

During certain alarm states and loopbacks, the DataSMART outputs an idle character on the DS0 channels assigned to the data port. This idle character is transmitted to the network and to the DTE attached to the port. You can specify the value of this idle character as 7E, 7F, or FF hex.

The default idle character is FF. This value should work correctly for most equipment. Some equipment may require 7E or 7F. These characters were chosen because FF is normally sent out by T1 equipment. It is also an abort character in HDLC, as is 7F. (They both have more than six consecutive ones.) The character 7E is the flag character (idle) in HDLC.

Using the command line

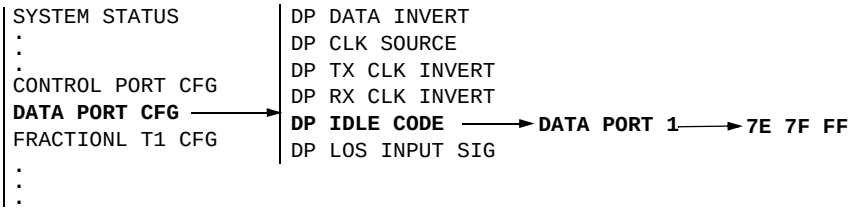
Use the **IDL** command to specify the idle character at the data port. You must have super-user or configuration privileges. The command syntax is:

IDL1:*cmd*

cmd Enter **7E**, **7F**, or **FF** to specify the idle character.

Using the front panel

To select the data port idle code from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until DATA PORT CFG appears in the display.
3. Push Select. DP DATA INVERT appears in the display.
4. Push Next or Previous until DP IDLE CODE appears in the display.
5. Push Select. DATA PORT 1 appears in the display.
6. Push Select. 7E 7F FF appears in the display. The currently configured value is blinking.
7. Push Next or Previous until the setting you want is blinking, then push Select.

Setting up DPLOS (data port loss of signal) processing

You can specify which signals are monitored for LOS at the data port. You can monitor the RTS signal, the DTR signal, both signals, or neither signal.

Data port LOS can be used to identify cases where the DataSMART and network are operating correctly, but the DTE has failed, has lost power, or has been disconnected.

When a data port LOS condition occurs, the DataSMART fills the network interface channels assigned to the data port with the idle character configured with the **IDL1** command for transmission toward the network. DP LOS is reported using the System Status (**S**) command (see "Examining system status" on page 135).

Using the command line

Use the **DPLOS** command to specify the signal(s) monitored for data port LOS. You must have super-user or configuration privileges. The command syntax is:

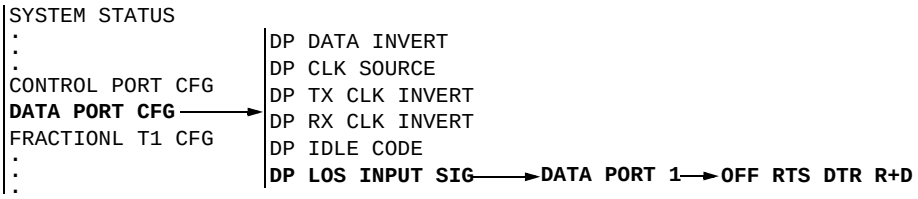
DPLOS1:*cmd*

cmd is one of the following:

R	Monitor RTS for LOS. This should work correctly with most equipment. Some equipment or cables may need a different setting.
D	Monitor DTR for LOS.
B	Monitor RTS and DTR for LOS. With this setting, the unit detects LOS if both RTS and DTR are low. If either signal is high, LOS is not detected.
N	Disable LOS monitoring. The DataSMART ignores RTS and DTR at the data port and assumes that the data port is connected and receiving valid data.

Using the front panel

To specify the signals being monitored for LOS, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until DATA PORT CFG appears in the display.
3. Push Select. DP DATA INVERT appears in the display.
4. Push Next or Previous until DP LOS INPUT SIG appears in the display.
5. Push Select. DATA PORT 1 appears in the display.
6. Push Select. OFF RTS DTR R+D appears in the display. The currently configured value is blinking.
7. Push Next or Previous until the setting you want is blinking, then push Select.

Assigning channels

The T1 line provides access to 24 DS0 channels on the network interface. You can assign some of these channels to the data port, assign others to the terminal interface, and leave other channels idle. One of the data port channels or idle channels can also be used for a data link to a remote unit. The DataSMART has two tables where you can keep separate configurations to handle differing demands on the T1 line.

Topics in this section

In this section, you'll find the following topics:

- "Planning the channel assignment" before setting up the unit, and why it's important
- "Methods of entering channels" — editing and loading channel configuration tables
- "Assigning network interface channels"— the most commonly used channel setups
- "Rules for assigning channels", "Assigning channels from the command line", and "Assigning channels from the front panel" — you'll need to read about these topics if you're not using one of the five typical channel setups

Planning the channel assignment

The T1 line has 24 channels you can assign to the terminal interface, data port, or idle.

In some simple cases, you may not need to plan the channel assignment. For example, the default configuration for add/drop units maps each network interface channel to its corresponding channel on the terminal interface. For DSUs without a terminal interface, every network interface channel maps to the data port by default.

NOTE
In more complex cases, it is important to have a channel assignment plan, especially when mapping channels to the data port. The DataSMART Configuration Worksheet in your installation guide can help you assign channels.

Consider these factors when assigning channels:

- If you are using a DS0 channel to support an IP management data link to a remote unit, include it in the plan. (The setups in "Assigning network interface channels" all use the IP data link on a DS0 and use the **NETIF** command to configure it; see "Selecting an IP network interface from the command line" on page 176.) The data link can use an idle channel or a data port channel. An error message is displayed if you attempt to assign the data link to a channel used by the terminal interface. Also, if the data link uses a data port channel, data port timing is disabled.

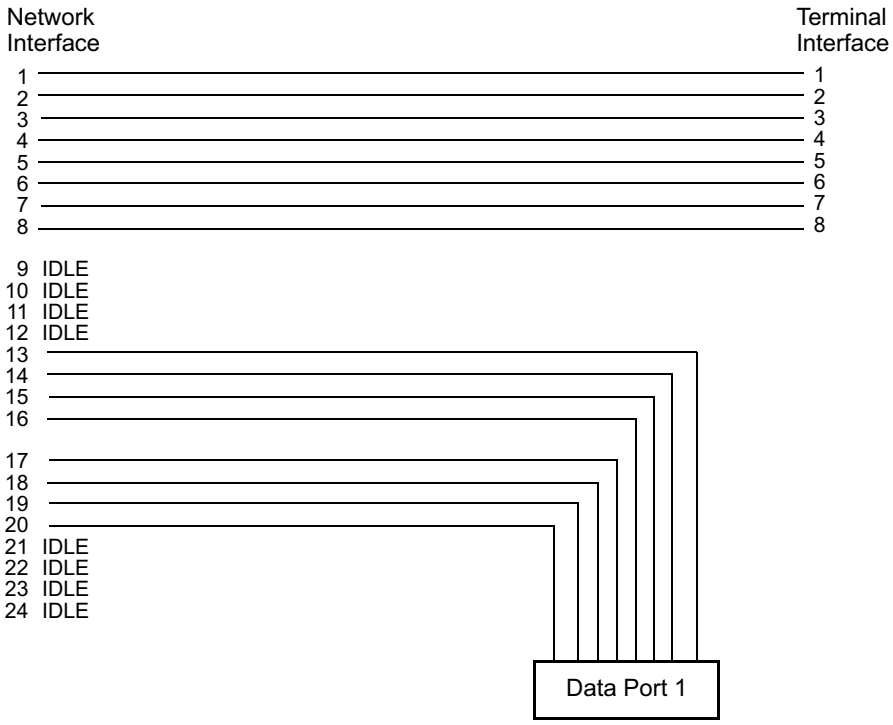
- In some rare cases, your configuration may not guarantee sufficient ones density at the network interface to avoid setting off alarms or losing synchronization. This might happen when your DTE is inactive, even though you haven't idled it. The solution may be to assign a set of alternating channels to the data port, and then configure the unassigned channels to outputting an idle code with high ones density.

NOTE

In a point-to-point connection, the units at both ends of the T1 line must have identical channel assignments. This is true regardless of your unit's channel assignment. Your network service provider may have to tell you what channel assignments to use.

Figure 6 shows a configuration that assigns channels 1-8 to the terminal interface and channels 13-20 to the data port, leaving the remaining channels idle. (This applies to add/drop units only; if your unit is a DSU without a terminal interface, you would leave channels 1-12 and 21-14 idle.) If the data port channels are configured to run at 64 Kbps, the data port speed is 8 x 64 = 512 Kbps.

Figure 6—Sample channel assignment



Methods of entering channels

You can assign channels using the command-line interface or the front-panel interface. There are some fundamental differences between the two methods:

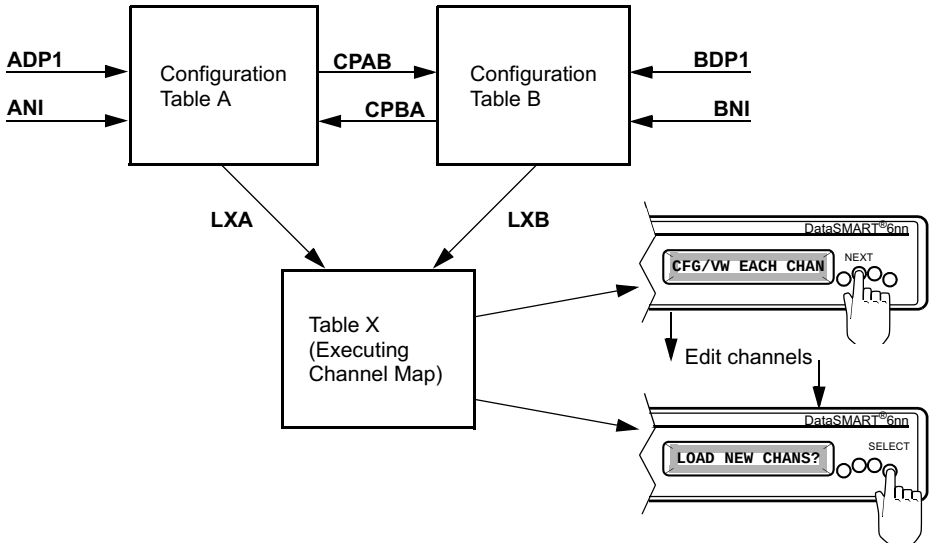
- When you use the front-panel interface, the changes you make are loaded directly into hardware.
- When you use the command-line interface, you are actually editing a table which you then load into hardware in a separate step.

The DataSMART has two tables, A and B, so that you can keep two separate configurations. This feature is useful at sites where, for instance, you have separate configurations for day-time and night-time traffic.

If you assign a channel configuration on the front panel, there is no way to later load it into one of the tables. If you make changes to the configuration using the front panel, it does not affect either of the tables.

Figure 7 illustrates how the configuration table editing commands and front panel editing affect the channel map used by the unit.

Figure 7—Flow chart for editing channel assignments



Editing configuration tables with the command line

The **ADP1** and **ANI** commands edit Configuration Table A.

The **BDP1** and **BNI** commands edit Configuration Table B.

The **CPAB** command copies Table A to Table B, and the **CBPA** command copies Table B to Table A.

Once Table A has been completely edited, the **LXA** command loads it into the executing channel map. The **LXB** command does the same for Table B.

Editing channel assignments with the front panel

For an overview of editing channel assignments with the front panel, see page 108.

Assigning network interface channels

The rest of this chapter contains network interface channel assignments for five typical DataSMART applications, as well as background on setting up a custom channel assignment. Record your application and channel assignment on the DataSMART Configuration Worksheet. Use the configuration procedure that applies to your application:

- All 24 channels, CSU using Robbed Bit Signaling; also called A-B bit or A-B-C-D bit signaling or Channel-Associated Signaling (CAS): see page 100.
- Channels 1-23, CSU using Robbed Bit Signaling; Channel 24, Data Port 1 @ 56 Kbps: see page 101.
- All 24 channels, CSU using Common Channel Signaling (CCS); Channel 24, also used for ISDN PRI or data equipment on terminal interface: see page 102.
- All 24 channels, Data Port 1 @1536 Kbps (24 x 64 Kbps); full rate DSU application: see page 103.
- Fractional T1 DSU @256 Kbps (4 x 64 Kbps): see page 104.
- None of the above: see "Rules for assigning channels" on page 105, "Assigning channels from the command line" on page 106, and "Assigning channels from the front panel" on page 108.

NOTE

When entering commands, be careful to distinguish between uppercase I and numeric 1. To see the syntax for these commands, enter the ***FC*** *command.*

Network management examples are in Chapter 8.

24-channel CSU, Robbed Bit Signaling (add/drop only)

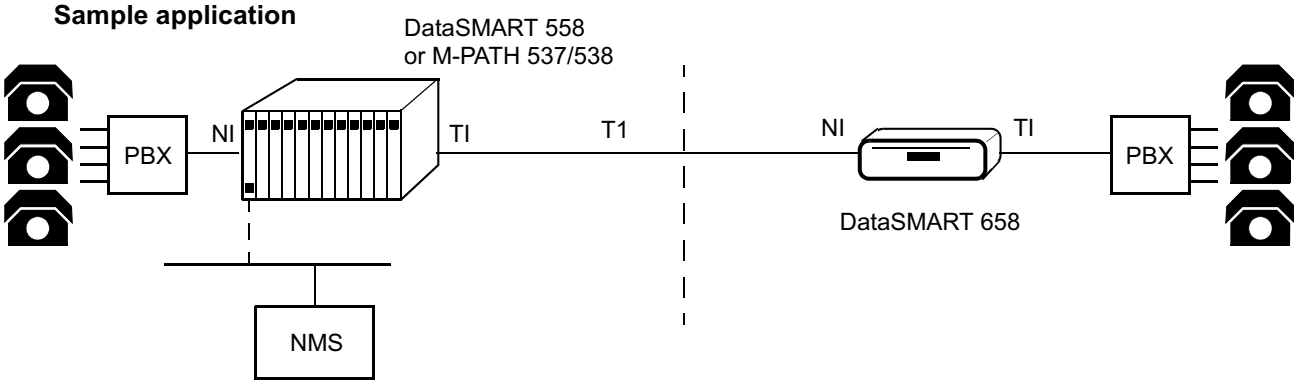
This application sets all 24 network interface channels to the terminal interface (voice-type channels). Use it if your terminal equipment requires the SF or ESF signaling bits.

In-band management to the remote site is available over the facility data link (FDL) only if the T1 service supports ESF end-to-end. Because all 24 channels are assigned to the terminal interface, this application cannot support a data link over a DS0.

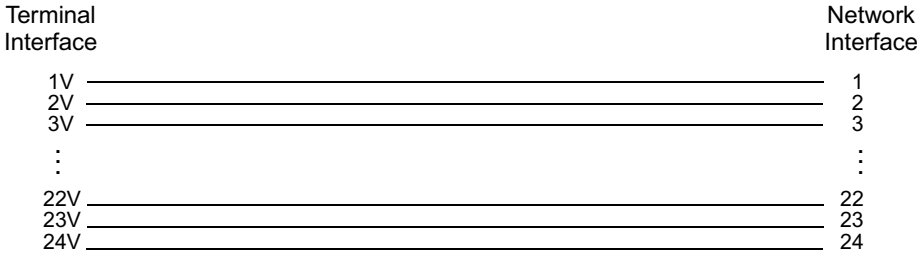
The near-end and far-end DataSMART units must have identical NI channel assignments.

Figure 8 —24-channel CSU, Robbed Bit Signaling

Sample application



Channel map diagram



- The **ANI1-24:V** command assigns NI channels 1-24 to the terminal interface, voice-type channels.

The procedure for configuring this application is in Chapter 6 of the installation guide.

23-channel CSU, Robbed Bit Signaling, 56 Kbps data port (add/drop only)

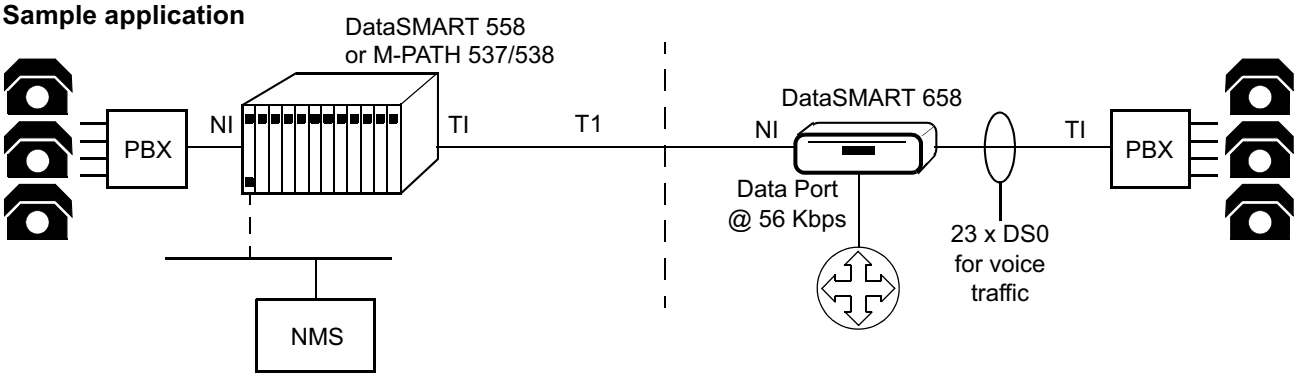
This application sets 23 network interface channels to the terminal interface (voice-type channels) and assigns Channel 24 to the DataSMART data port at 56 Kbps. Use it if your terminal equipment requires the SF or ESF signaling bits.

This application can support data-link management over channel 24.

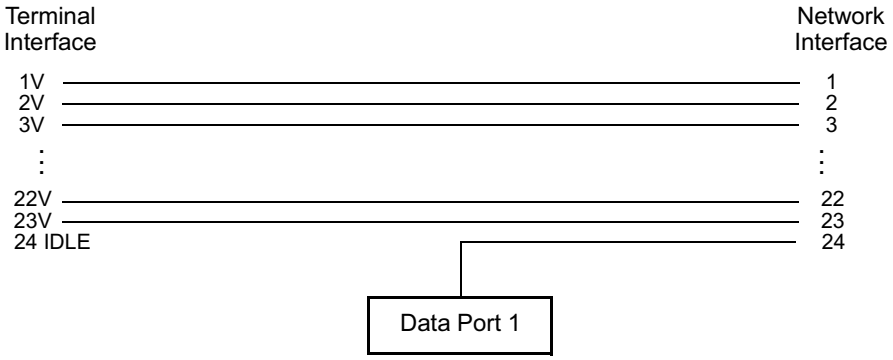
The near-end and far-end DataSMART units must have identical NI channel assignments.

Figure 9 —23-channel CSU, Robbed Bit Signaling, 56-Kbps data port

Sample application



Channel map diagram



- The **ANI1-23:V** command assigns network interface channels 1-23 to the terminal interface, voice-type channels.
- The **ADP1:56,24** command assigns network interface channel 24 to the data port at 56 Kbps.

The procedure for configuring this application is in Chapter 6 of the installation guide.

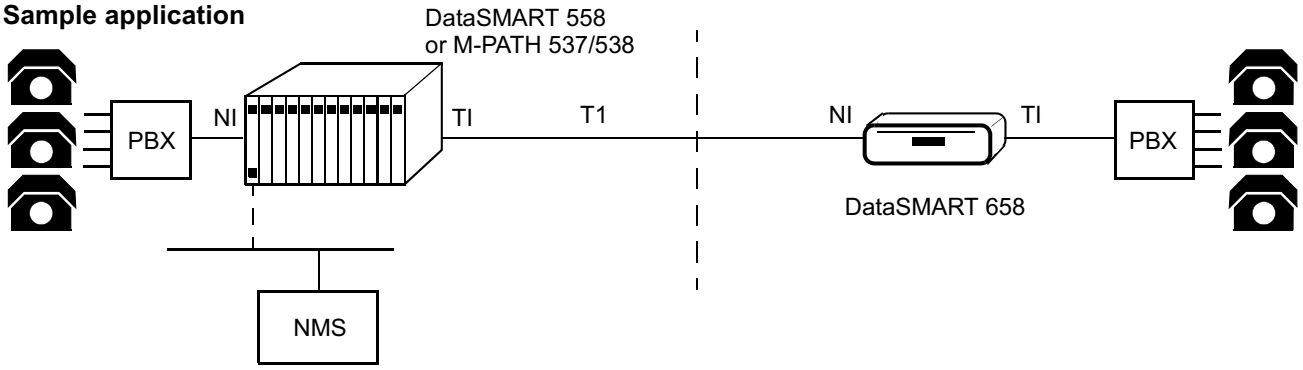
24-channel CSU, Common Channel Signaling (add/drop only)

This application sets all 24 network interface channels to the terminal interface (data-type channels). Use it for Common Channel Signaling (CCS) or ISDN PRI applications, if you have data equipment on the terminal interface, or if a clear channel is required. Because all 24 channels are assigned to the terminal interface, this application can not support a data link over a DS0.

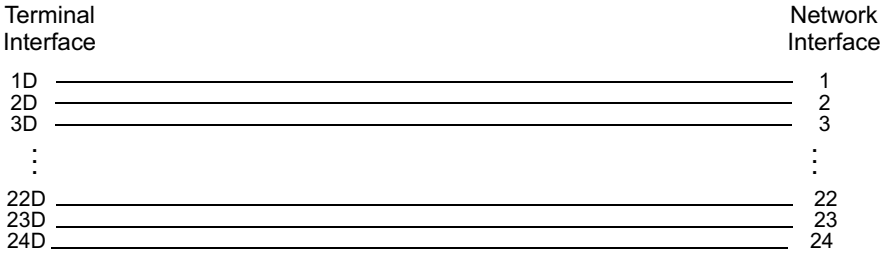
The near-end and far-end DataSMART units must have identical NI channel assignments.

Figure 10 —24-channel CSU, Common Channel Signaling

Sample application



Channel map diagram



- The **ANI1-24:D** command assigns NI channels 1-24 to the terminal interface, data-type channels.

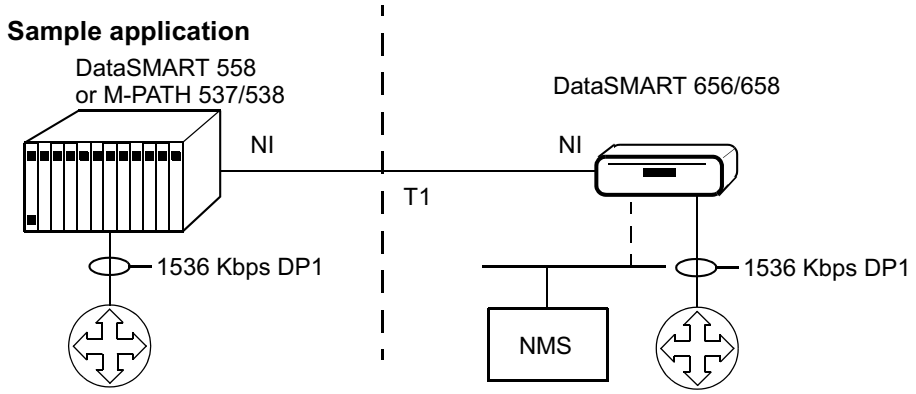
The procedure for configuring this application is in Chapter 6 of the installation guide.

24-channel Full Rate DSU, 1536 Kbps

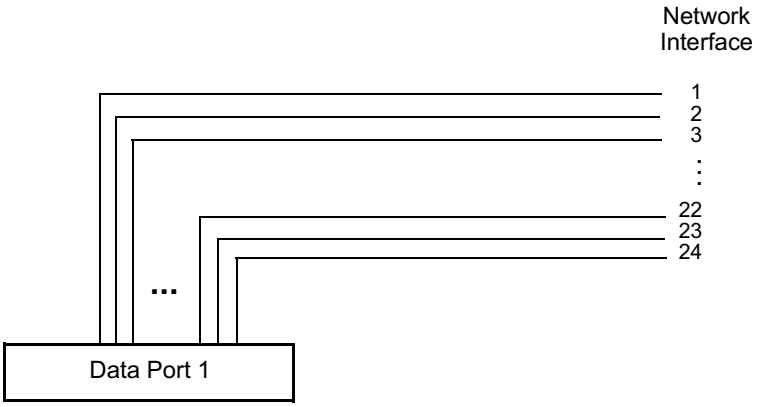
This application assigns all 24 network interface channels to the data port. All channels are set to 64 Kbps for a total of 1536 Kbps at the data port.

The near-end and far-end DataSMART units must have identical NI channel assignments.

Figure 11—24-channel Full Rate DSU, 1536 Kbps



Channel map diagram



- The **ADP1:64,1-24** command assigns network interface channels 1-24 to the DataSMART unit's data port at 64 Kbps.

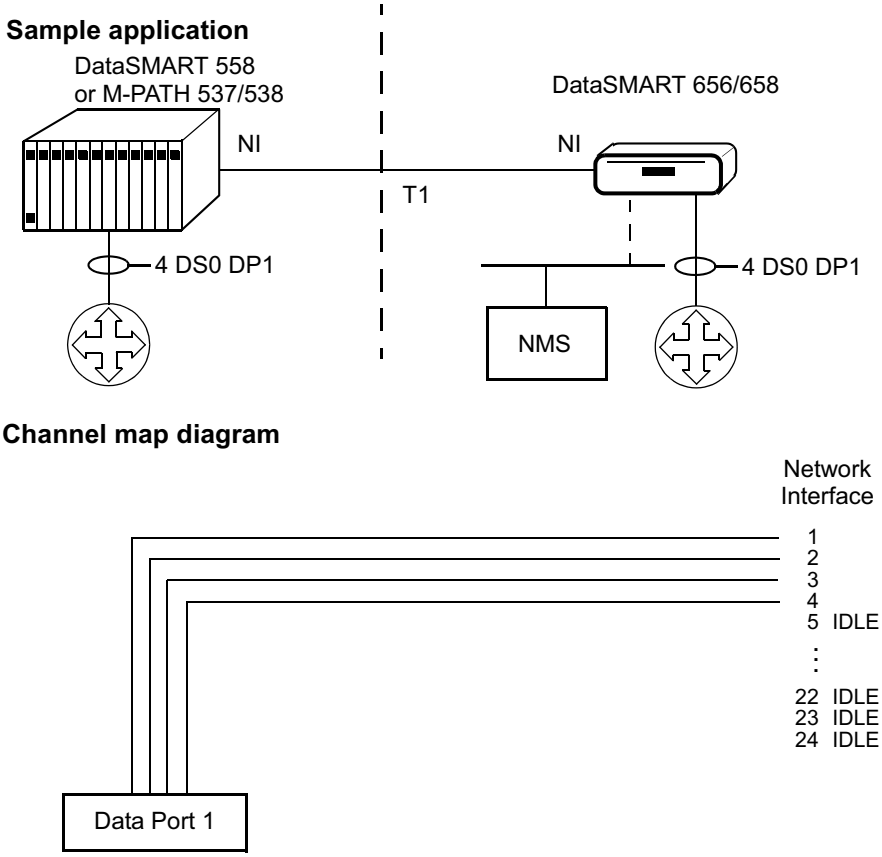
The procedure for configuring this application is in Chapter 6 of the installation guide.

Fractional T1 DSU, 256 Kbps

This application assigns network interface channels 1-4 to the data port. Each data port channel is set to 64 Kbps for a total of 256 Kbps at the data port. All other channels are idle.

The near-end and far-end DataSMART units must have identical NI channel assignments.

Figure 12—Fractional T1 DSU, 256 Kbps



- The **ADP1:64,1-4** command assigns network interface channels 1-4 to the DataSMART unit's data port at 64 Kbps.
- The **ANI5-24:I** command sets NI channels 5-24 to idle.

NOTE

*To assign more or fewer channels to the data port, modify the above commands. For example, to assign eight channels to the data port, the commands are **ADP1:64,1-8** and **ANI9-24:I**.*

The procedure for configuring this application is in Chapter 6 of the installation guide.

Rules for assigning channels

Rules for assigning data port channels

When assigning network interface channels to the data port and the terminal interface, the channels for the data port must be grouped. Within the group, the channels can be contiguous or alternating. If the channels in the group are alternating, the intervening channels are assigned to idle.

For instance, if data port 1 has eight channels to assign, you can assign them in a single group of contiguous channels (1-8), but not two groups on contiguous channels (1-4 and 10-13). Or, if you want to use alternating channels, you can assign them to a single group of alternating channels (2, 4, 6, 8, 10, 12, 14), but not to two groups of alternating channels (2, 4, 6, 8 and 14, 16, 18, 20).

The TI idle code, which goes out the terminal interface on all idle channels, MUST contain sufficient ones to keep the circuit synchronized. When you specify the idle code, make sure you select a code with sufficient ones. (See "Specifying TI idle code" on page 84.)

NOTE

Besides assigning the channels, you must also specify the data rate for the data port. See "Assigning DS0 lines to a port" on page 106.

Rules for assigning terminal interface channels

The rules for channel assignments between the network interface and the terminal interface are:

1. The channel number on the TI side must match the channel number on the NI side.
2. If equipment connected to the TI requires the super frame signaling bits or the extended super frame signaling bits to be passed through the DataSMART DSU, set the channel type to V (voice).
3. If the equipment connected to the TI requires a 64 Kbps clear channel (no signaling bits), set the channel type to D (data).
4. You do not need to group the TI channels in any special way, as is the case with data port channels.
5. If you use an alternating scheme, you can assign a single data port channel to a channel in between two TI channels.

Compatible and incompatible configurations

The following formats and settings usually go together:

- Super frame, AMI, 56 Kbps channel data rate, one channel on the data port.
- Extended super frame, B8ZS, 64 Kbps channel data rate, aggregated channels on the data port.

The following format-and-setting combination is *not* recommended:

- AMI, 64 Kbps channel data rate (this does not guarantee ones density on the T1 line).

Assigning channels from the command line

You set channel bandwidth using the commands listed in the Fractional T1 Configuration menu. To display this menu, enter **FC**.

```
                FRACTIONAL T1 CONFIGURATION MENU

<table>DP<port>:<rate>[,<nicn>]
                    - DP=Assign NI Channel Map for Data Port
     table A/B      - Tables A or B Containing Channel Assignment
     port  1        - Data Port Number
     rate  56/64    - Channel Rate in 1000 bps
     nicn  1 .. 24  - NI Channel numbers assigned to Data Port or
           1,3,5,...- Can be alternating DS0 channel numbers or
           1-24     - a contiguous range.

<table>NI<nicn>:<ticn>,<nicn>:<ticn>, ...
                    - NI=Assign NI Channels to IDLE
     table A/B      - Tables A or B Containing Channel Assignment
     nicn  1 .. 24  - NI Channel numbers
     ticn  I        - I for Idle

CPAB / CPBA         - Copy A to B or B to A
LXA  / LXB          - Load and Execute Table A or B
TAV  / TBV          - View Table A or B
TXV                 - View Executing Channel Assignment
```

Assigning DS0 lines to a port

This command allows you to edit data port channel assignments and data rates in table A or table B. You must have super-user or configuration privileges to use this command.

NOTE

*Use a numeric **1** (not an uppercase **I**) in the **ADP1** and **BDP1** commands.*

*table***DP1:***rate*[,*nicn*]

table	Specify **A** or **B** to indicate which table you want to edit.
rate	Specify either **56** or **64** Kbps.
nicn	Specify the NI channels that you want to assign to the data port, where *nicn* is one of the following: A single channel number (for example, **11**). A range of channel numbers, delimited by a dash (for example, **2-8**). A series of odd or even channel numbers, delimited by commas (for example, **7,9,11** or **10,12,14**).

Assigning network channels to the terminal interface or IDLE

Use this command to:

- Assign network (NI) channels to the terminal interface (TI) — add/drop only
- Idle out unused channels on the NI
- Assign “voice” or “data” type to TI channels — add/drop only

Note that the assignments must be “straight across”; the NI channel must go to the TI channel of the same number.

NOTE

You cannot assign the data link to a remote DataSMART unit over a channel that is assigned to the terminal interface.

You must have super-user or configuration privileges to use this command.

*table***NI***ni_channel:[d,v,i]*

*table***NI***ni_channel_range:[d,v,i]*

*table***NI***ni_single_channel:[d,v,i]*

table	Specify **A** or **B** to indicate which table you want to edit.
ni_channel_range	Specify a range of NI channels, delimited by a dash.
single_channel:i	Set a single channel to idle. For instance, **3:i** idles NI channel 3.

Viewing the contents of table A and B

You can inspect the contents of the tables by using the **TAV** and **TBV** commands. You must have super-user or configuration privileges.

TAV	Display the contents of table A.
TBV	Display the contents of table B.

The **TXV** command shows the current assignments. **TXV** does not require any privileges to use.

TXV	Display the current channel assignments on the DataSMART.

To look at table A, for example, enter the **TAV** command from any prompt. The table A report will look something like the display shown below. (The same channel assignment is illustrated in Figure 6 on page 97.) The report displays the mapping of NI channels in two different ways. The top of the report lists the ports in the left column and shows rate and all channels assigned to that port to the right. The bottom of the report lists every channel and shows its assignment and whether it is configured for idle or mapped to the data port.

Configuring the interfaces from a table

These commands load a configuration from a table into the hardware, which then operates as configured. You must have super-user or configuration privileges.

LXA	Load configuration from Table A.
LXB	Load configuration from Table B.

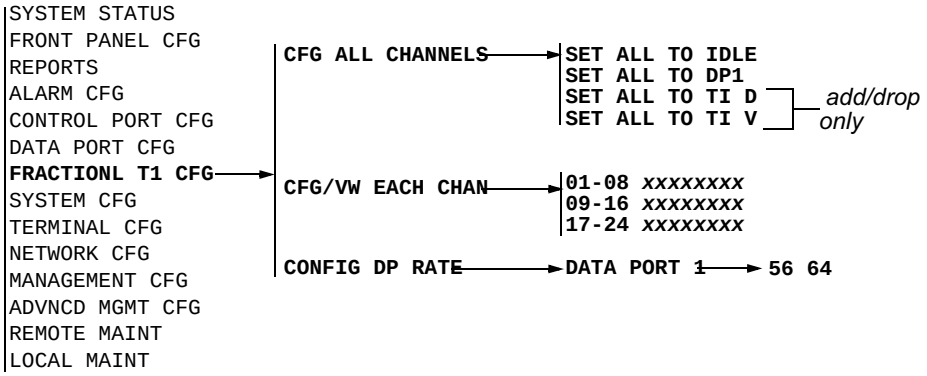
Copying one table into another

You can copy the contents of one table into the other table using the **CPAB** and **CPBA** commands. You must have super-user or configuration privileges.

CPAB	Copy Table A to Table B.
CPBA	Copy Table B to Table A.

Assigning channels from the front panel

The commands available for assigning channels from the front panel are shown below.



Using the CFG ALL CHANNELS command

This command is designed to simplify configuring channels from the front panel. For example, if you plan to configure your unit with most channels going to the terminal interface (voice), you could use SET ALL TO TI V. This assigns every channel to TI V. Then you could use CFG/VW EACH CHAN to selectively change the other channels.

The steps for setting all channels are:

1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until FRACTIONL T1 CFG appears in the display.
3. Push Select. CFG ALL CHANNELS appears in the display.
4. Push Select. SET ALL TO IDLE appears in the display.
5. Push Next or Previous until the desired setting appears in the display, then push Select.

Using the CONFIG DP RATE command

Use this command to configure the data port DS0 channel data rate for the data port.

1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until FRACTIONL T1 CFG appears in the display.
3. Push Select. CFG ALL CHANNELS appears in the display.
4. Push Next or Previous until CONFIG DP RATE appears in the display.
5. Push Select. DATA PORT 1 appears in the display.
6. Push Select. 56 64 appears in the display. The currently configured value is blinking.
7. Push Next or Previous to change to the desired value, then push Select.

Using the CFG/VW EACH CHAN command

Use this command to assign or reassign from one to eight channels at a time. You can also use this command to view the channel assignments from the front panel.

NOTE

The channel configuration display on the LCD is not updated dynamically, If another person is logged into the DataSMART and changes a channel configuration while you are displaying the channel configuration on the LCD, you will not see the changes until the next time you select CFG V/W EACH CHAN.

To view or change the channel assignments, follow these steps.

1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until FRACTIONL T1 CFG appears in the display.
3. Push Select. CFG ALL CHANNELS appears in the display.
4. Push Next or Previous until CFG V/W EACH CHAN appears in the display.
5. Push Select. A display similar to the following appears, with the characters 01-08 blinking:

   ```
   01-08 IIIIIIII
   ```

   The above example shows that channels 01-08 are set to idle. If channels 01-04 were assigned to the data port, the display would show this:

   ```
   01-08 1111IIII
   ```

   The letters that indicate the channel settings can be numeric 1 (for data port 1) or uppercase I (for idle).
6. If you want only to view the channel settings, push Next or Previous to see channels 09-16 and 17-24. If you want to change a channel assignment, go to step 7.
7. To change a channel assignment, push Select. The channel range stops blinking and an underline appears under the first channel letter.
8. Push Next or Previous to move the underline to the letter that represents the channel you want to change. (Channel assignments do not have to be contiguous.) For instance, to change channel 2, the display should look like this:

   ```
   01-08 II_IIIII
   ```
9. Push Select. The underline disappears and the letter begins to blink.
10. Push Next or Previous to change the letter to the setting you want.
11. Push Select. The letter stops blinking and the underline reappears.
12. Repeat steps 8 through 11 until channels 01-08 are changed to the desired settings.
13. Push Escape. In the display “01-08” will begin to blink. You can now use Next or Previous to switch to ranges 09-16 and 17-24.
14. Push Next or Previous to switch to the other ranges as desired, and repeat steps 7 through 13.
15. When all channels are set as desired, push Escape. A query will ask “LOAD NEW CHANS?” Push Select to load the new channels, or push Escape to exit without making any changes. If you pushed Select, “CHANNELS LOADED” appears in the display.

C H A P T E R

6 Performance monitoring

This chapter describes how the DataSMART unit's performance monitoring facilities help troubleshoot network problems. The DataSMART provides a statistical report and detailed performance reports at the physical (T1/FT1) level. It also provides history reports for alarms and security violations.

Report types and their common uses

This report type...	includes...	which allow you to...
T1 statistical report	NI Statistical Performance report (**NSR**)	Quickly identify T1 receive-line problems when turning up T1 service.
	TI Statistical Performance report (**TSR**)	Quickly identify T1 receive-line problems on the customer premise equipment (CPE) when turning up T1 service. (Available on add/drop units only.
T1 performance reports	User NI performance reports (**UNSR/UNLR**)	Identify T1 receive-line quality problems over a longer time frame than the NSR.
	User TI performance reports (**UTSR/UTLR**)	Identify T1 receive-line quality problems on the CPE over a longer time frame than the TSR. Available on add/drop units only.
	Far-end performance reports (**FESR/FELR**)	Identify T1 transmit-line quality problems
	Carrier NI performance reports (**CNSR/CNLR**)	Monitor the carrier T1 performance registers.
History reports	Alarm History report (**AHR**)	View the 20 most recent T1 alarm messages.
	Security History report (**SHR**)	View the 10 most recent security violations.

The first section of this chapter shows how to access the various command-line reports. The next sections show how to interpret the command-line reports, and the final section shows how to access and interpret reports from the front panel.

Accessing the reports

The Reports menu lists commands for accessing reports.

To see the list, enter **R** at the command line.

DataSMART 658 only

DataSMART 658 only

```
                    REPORTS MENU

UNSR / UNLR       - User NI Short/Long Performance Report
UTSR / UTLR       - User NI Short/Long Performance Report
CNSR / CNLR       - Carrier NI Short/Long Performance Report
FESR / FELR       - Far End PRM Short/Long Performance Report

NSR:[z]           - User NI Statistical Performance Report
TSR:[z]           - User TI Statistical Performance Report
                    z = Display Report then Zero Counts (Optional)
AHR               - Alarm History Report
SHR               - Security History Report

PL:<len|style>    - Set Page Length, <len> = 20 .. 70 (or 0 = Off), or
                    <style> = P (Page Break), M (More), or V (View)
```

TIP
The reports are also available using the SMARTools Installer application shipped with your DataSMART unit.

To display any report, simply enter the appropriate command from the command line. You do not need any special privilege level.

Most reports have a long or short version. The long version differs from the short version only in that it includes a breakdown of the performance information for the previous 24 hours, shown in 15-minute intervals.

TIP
For information on these and other reports, see the sections on interpreting performance reports starting on page 114.

For example, use these commands to display the User NI reports.

UNSR Display the short version of the User NI report.

UNLR Display the long version of the User NI report.

Using the Z option with the NSR and TSR commands

The NI and TI Statistical reports provide performance data similar to the NI User report, plus in-service data about total errors counted at the network interface. By using the **Z** option with these report commands, you can clear the error counts whenever the report is displayed. This way, the next time you display the report it will show just the errors accumulated since the last time you displayed the report.

The command syntax is:

NSR [**Z**]

TSR [**Z**]

Z Clears the error counts from the report, once the report is displayed.

Formatting the reports

The **PL** command formats all the reports, either for a printer or a terminal. You can set the page length and select either "page break" for output to a printer, or "more prompt" for output to a screen. A page length of 0 disables both page breaks and prompting.

By default, no page length is specified and page breaks and prompting are disabled. If you enter a page length, the command defaults to a "more prompt" (**M**) unless you specify "page breaks" (**P**).

The **PL** command syntax is:

PL:*len*|*style*

len	Specify the page length as **0**, **20** ... **70**. 0 disables page breaks and prompting.
style	Specify **P** for "page break," **M** for "more prompt," or **V** to display the current settings without changing anything.

For example, to fit a report on a 22-line monitor, enter:

PL:22:M

Any time you change the length or style parameter, a display will show the state of the settings after the change.

Clearing the performance database

There are six actions you can take that will clear report data.

Resetting the date or time on the DataSMART using the **ST** or **SD** commands (see "Setting date and time" on page 38) clears the performance data and resets counters. Using the **ZALL** command (see "Zeroing all counters" on page 49) has the same effect, without changing the time.

The **SD**, **ST**, and **ZALL** commands clear data from all reports except the Carrier NI reports, the Alarm History report, and the Security History report.

The following actions will clear data from all reports, including the Carrier NI and history reports:

- Cycling power to the DataSMART
- Using the **BOOT** command (see "Obtaining new system software" on page 50)
- Resetting the DataSMART to its defaults with the **RSD** command (see "Resetting to default values" on page 52). This command causes you to lose the current alarm history data, performance data, and configuration settings. Use the **RSD** command with caution.

Interpreting the NI and TI Statistical reports

*The **NSR** and **TSR** commands display Statistical reports of the received signal on the network interface and terminal interface respectively. The **NSR Z** and **TSR Z** commands also display Statistical reports, and then clear the error data.*

Using the NI Statistical report when you first turn up a new T1 line will give you a snapshot of T1 service quality in the receive direction. For more detail, run the User NI performance reports (see page 118). The TI Statistical Report is similar. It shows the quality of the connection to customer premise equipment connected to the DataSMART.

A Statistical report has two parts. The first part is a statistical summary of the recent performance history of the received signal. The second part is an in-service performance measurement of the received signal. The following figure shows an example of an NI Statistical report (**NSR**).

```
KENTROX DataSMART - USER NI STATISTICAL PERFORMANCE REPORT
ADDRESS: 00:00:000              NAME: PORTLAND,OR
DATE: FEB 14, 1997              TIME OF DAY: 16:48
            |-------------- G.821 ---------------|
            %AS    %EFS     %ES    %SES     %DM    %BES    %CSS
            ------  ------  ------  ------  ------  ------  ------
CUR 15-MIN  100.00  100.00  0.0000  0.0000  0.0000  0.0000  2.0304
PRE 15-MIN  98.888  99.775  0.2247  0.0000  6.6666  0.2247  2.0224
CUR 24-HR   99.073  99.439  0.5609  0.4861  2.2222  0.0747  3.4779
START OF TEST:  DATE: FEB 14, 1997
                TIME: 16:00
PERFORMANCE MEASUREMENT            COUNT
-----------------------------   ----------
ESF ERRORS                         11718
CRC6 ERRORS                         3693
OUT OF FRAME ERRORS                 8025
FRAME BIT ERRORS                      18
BIPOLAR VIOLATIONS                 14175
CONTROLLED SLIPS                     155
YELLOW ALARM EVENTS                    0
AIS EVENTS                             0
LOSS OF FRAME EVENTS                   1
LOSS OF SIGNAL EVENTS                  3
```

What to look for

To test NI performance for a specified time period, use the **NSR Z** command to generate a report and clear the data. Then periodically use the **NSR** command to check performance over time. Trouble indicators are:

- Values in the %AS and %EFS columns that are under 100 percent
- Nonzero values in the %ES, %SES, %DM, %BES, and CSS columns
- Nonzero counts in the Performance Measurement area (for definitions of the performance measurements, see "Interpreting the NI and TI Statistical reports" on page 114)

The report's statistical summary

The statistical summary shows statistical percentages for the current 15-minute interval, the previous 15-minute interval, the current 24-hour interval, and each of the last seven days. These intervals are the same as those in the User NI report; see "Time intervals in the performance report" on page 119 for a description of them.

The percentages are computed from the counts stored in the performance database for the User NI report. They are computed using the concept of an "available second". In the formulas defined below, you will see the variable "Sec_avail". An available second is simply any second that is not an unavailable second:

Sec_avail = Sec_total - UAS

Specifically, the number of available seconds for any time period is simply the number of total seconds for the time period (900 for 15 minutes, 86400 for 24 hours) minus the number of UAS seconds. See "UAS" on page 120 for a definition of an unavailable second.

Any time "Sec_avail" is zero for a time period and the formula for computing the percentage uses "Sec_avail" in a denominator, a series of dashes is displayed as the result instead of a numerical value.

The following is a list of the seven fields in the statistical summary and the formulas used to compute their values.

Field header	Description
%AS	This field lists the percentage of available seconds (%AS) for the time interval. The formula for this statistic is: %AS = (Sec_avail / Sec_total) x 100
%EFS	This field lists the percentage of error-free seconds (%EFS) for the time interval. An error-free second is any available second that was not an errored second. The formula is: %EFS = ((Sec_avail - ES) / Sec_avail) x 100 where ES is the number of errored seconds for the time interval.
%ES	This field lists the percentage of errored seconds (%ES) for the time interval. The formula for this statistic utilizes ES, where ES is the number of errored seconds. The formula is: %ES = (ES / Sec_avail) x 100 Note that the sum of %EFS and %ES should be 100%.
%SES	This field lists the percentage of severely errored seconds (%SES) for the time interval. The formula for this statistic utilizes SES, where SES is the number of severely errored seconds (using the same definition as for the User NI report; see page 120). The formula is: %SES = (SES / Sec_avail) x 100
%DM	This field lists the percentage of degraded minutes (%DM) for the time interval. The formula for this statistic utilizes DM, where DM is the number of degraded minutes (using the same definition as for the User NI report; see page 120). The formula is: %DM = (DM / ((Sec_avail / 60) rounded to next higher integer)) x 100
%BES	This field lists the percentage of bursty errored seconds (%BES) for the time interval. The formula for this statistic utilizes BES, where BES is the number of bursty errored seconds for the time interval (using the same definition as for the User NI report; see page 120). The formula is: %BES = (BES / Sec_avail) x 100
%CSS	This field lists the percentage of controlled slip seconds (%CSS) for the time interval. The formula for this statistic utilizes CSS, where CSS is the number of controlled slip seconds for the time interval (using the same definition as for the User NI report; see page 120). The formula is: %CSS = (CSS / Sec_avail) x 100

The Statistical report's in-service performance measurement

The second part of the report displays counts of various error conditions in the received network signal. These are just raw counts, not percentages. The data for this display is kept in registers separate from the registers used for other reports. You can reset the counts at any time. Resetting the count does not affect performance information (including the information in the first part of the Statistical report). The error counts are useful for running an in-service test on the network line.

To run an in-service test on the network interface, use these steps:

1. Issue the **NSR** or **TSR** command using the **Z** option to clear (zero-out) the error counts.

   NSR Z

   This displays the Statistical report, showing the error counts at the time the command was issued, and then clears the error data.

2. Wait the desired time interval.

3. Issue the command again.

   This displays the error counts accumulated since the time you cleared the error counts.

   The figure below shows an example of an in-service performance measurement. The header shows the start of the test, which is the time that the error counts were last cleared. Below that are two columns, listing the type of error condition and a corresponding error count. The maximum value that may appear in any count field is 2^{32}-1 (4,294,967,295). When this limit is reached, the count wraps to zero (0).

```
KENTROX DataSMART - USER NI STATISTICAL PERFORMANCE REPORT
ADDRESS: 00:00:000              NAME: PORTLAND,OR
DATE: FEB 14, 1997              TIME OF DAY: 16:48
            |-------------- G.821 ---------------|
            %AS    %EFS     %ES    %SES     %DM    %BES    %CSS
            ------  ------  ------  ------  ------  ------  ------
CUR 15-MIN  100.00  100.00  0.0000  0.0000  0.0000  0.0000  2.0304
PRE 15-MIN  98.888  99.775  0.2247  0.0000  6.6666  0.2247  2.0224
CUR 24-HR   99.073  99.439  0.5609  0.4861  2.2222  0.0747  3.4779
START OF TEST:  DATE: FEB 14, 1997
                TIME: 16:00
PERFORMANCE MEASUREMENT            COUNT
-----------------------------   ----------
ESF ERRORS                          13016
CRC6 ERRORS                         11215
OUT OF FRAME ERRORS                  2105
FRAME BIT ERRORS                       18
BIPOLAR VIOLATIONS                  14175
CONTROLLED SLIPS                      155
YELLOW ALARM EVENTS                     0
AIS EVENTS                              0
LOSS OF FRAME EVENTS                    1
LOSS OF SIGNAL EVENTS                   3
```

Interface Statistical report

Counts of the following error conditions are maintained and displayed in response to the **NSR** or **TSR** command:

- ESF Errors (ESF only): this event occurs when a frame contains a CRC error, an OOF error, or both.
- CRC6 Errors (ESF only): this error occurs when the CRC checksums calculated for a frame at the transmitting and receiving ends are different.
- Out of Frame Errors (ESF and SF): two or more framing bit errors have been received within a 3-millisecond period.
- Frame Bit Errors (ESF and SF): errors have been received in the framing bits at a rate of less than 1 every 3 milliseconds.
- Bipolar Violations (ESF and SF): this event is any bipolar violation generated in error (not including intentional bipolar violations generated by B8ZS coding).
- Controlled Slips: this event is the addition or deletion of a single frame in the received data stream, due to a timing difference of exactly one frame between the transmitted and received data streams. Make sure you are using one and only one timing source.
- Yellow Alarm Events: this event is a transition from the condition of "not receiving yellow" to the yellow condition.
- AIS Events: this event is a transition from the condition of "not receiving AIS" to the AIS condition.
- Loss-of-Frame Events: this event is a transition from the framed condition to the OOF condition.
- Loss-of-Signal Events: this event is a transition to the LOS condition. See "Examining system status" on page 135.

For more detailed definitions, see page 120, "Troubleshooting tree" on page 140, or the Glossary.

Interpreting the User NI and User TI reports

The DataSMART monitors the received signal on a T1 line. The User NI report displays error counts and can be used to determine signal quality.

The DataSMART monitors the received signal on a T1 line for a variety of different error conditions (see "T1 alarms and signal processing" on page 214 for descriptions of errored signal conditions). The DataSMART counts the errors and then uses the count to determine the quality of the 1-second interval during which the errors occurred.

For each time interval, the DataSMART tallies the counts and displays the information in the reports. The reports also show the error conditions and whether or not an alarm was present.

The following figure is an example of the User NI Short Performance Report (**UNSR**). The **UTSR** report is very similar.

```
KENTROX DataSMART - USER NI SHORT PERFORMANCE REPORT
ADDRESS: 00:00:000              NAME: PORTLAND,OR
DATE: FEB 14, 1997              TIME OF DAY: 16:44
STATUS CODES: C=CRC6, B=BPV, L=LOS, O=OOF, E=EER, A=AIS, Y=YEL,
              @=ALARM ACTIVE, T=TEST ACTIVE
SECOND OF INTERVAL: 881 OF 900  COMPLETED INTERVALS: 2 OF 96

                    G.821         G.821  G.821        G.821
              EE      ES    BES    SES    UAS    CSS    DM     STATUS
           ------  -----  -----  -----  -----  -----  ----  ---------
CUR SEC         0      0      0      0      0      0     0      E  @
PRE SEC         0      0      0      0      0      0     0      E  @
CUR 15-MIN   3710      2      2      0     10     18     1  CB  E  @
PRE 15-MIN     18      5      0      5     15     16     0   BL E  @
CUR 24-HR      80     13      0     13     15     75     0  CBLOE  @
```

What to look for

Real or potential problems with T1 service are indicated by:

- Nonzero results in the performance measurement columns (EE, ES, BES, SES, UAS, CSS, and DM) indicate seconds (or minutes) when errors occurred.
- Letters in the Status column indicate error conditions, and the @ character appears if the error conditions persisted long enough to cause alarms.

For details, see page 120.

Time intervals in the performance report

The report shows the performance data for the current second, the previous second, the current 15-minute period, the previous 15-minute period, the current day, and the previous seven days.

Each day is broken into ninety-six 15-minute intervals. Interval one starts at 00:00 (midnight), interval two at 00:15, interval three at 00:30, and so on.

CUR 15-MIN refers to the performance data tabulated so far for the 15-minute interval. For instance, in the previous figure, the third row shows the performance for the 15-minute interval starting at 00:15 (notice that the time of day is 00:27).

Each 15-minute interval consists of 900 seconds. The field in the header labeled "SECOND OF INTERVAL" shows how many seconds into the interval the measurement extends. In the example, the data has been collected for 757 seconds of the current interval.

In a report, CUR 24-HR refers to a rolling 24-hour period. In other words, it is the previous ninety-six 15-minute intervals. The field labeled "COMPLETED INTERVALS" indicates whether or not the DataSMART has been running for the full ninety-six intervals that make up a 24-hour day. Unless the DataSMART was recently restarted, the completed intervals display should always read "96 OF 96." The 24-hour count may show less than ninety-six 15-minute intervals if it was cleared within the last 24 hours.

The report also shows the performance data for each of the last seven days, if the DataSMART has been powered up for seven days; otherwise, it shows the data collected since the DataSMART was last powered up. For instance, if the DataSMART has only been powered up for 48 hours, the report will only have a listing for two days, since only two days have been completed so far.

If one of the time intervals shows a row of dashes (-), that means that either the DataSMART was powered down during that period or data has not yet been collected for that period.

A zero (0) indicates that the unit was collecting data and for that field the count was zero.

Time intervals and the long report

The long report (use the **UNLR** or **UTLR** command) shows the same information as the short report and also includes performance data for each complete 15-minute interval in the current 24 hours (that is, the previous ninety-six 15-minute intervals). If not all of the 15-minute intervals are listed, it means the DataSMART has not been on for 24 hours. A dash displayed in a field means that the unit was powered down for that period.

The following figure shows the additional information provided by the long version of the User NI report (**UNLR**).

```
TIME ACCUMULATED
    17:30        0      0      0      0      0      0     0
    17:15        0      0      0      0      0      0     0
    17:00        0      0      0      0      0      0     0
    16:45        0      0      0      0      0      0     0
    16:30       18      5      0      5     15     16     0   BL E  @
    16:15       62      8      0      8      0     59     0  C LO   @
```

For each time interval there are eight types of performance measurements. These measurements are described below.

Field header	Definition
EE	This field shows the number of error events (EEs) that have occurred, up to a maximum of 999,999. If the line uses ESF framing, the following error conditions cause a single EE to be counted: a transition to the LOS condition a transition to the AIS condition a transition to the OOF condition a second with a controlled slip (also referred to as a frame slip)[1] a BPV error a CRC6 error If the line uses SF framing, an EE is the number of BPVs per second.
ES	This field lists the number of errored seconds (ESs) that have occurred. If the line uses ESF framing, an ES is any second that is not a UAS that contains: an LOS condition, or an AIS condition, or an OOF condition, or one or more CRC6 or BPV errors. If the line uses SF framing, an ES is any second with a BPV, LOS, AIS, or OOF. Note that controlled slips do not result in ESs (as per CCITT G.821 paragraph 1.8). Also note that when a single LOS, AIS, or OOF condition lasts for several seconds, it counts as a single EE, not as several ESs and SESs.
BES	This field lists the number of bursty errored seconds (BESs) that have occurred during the time interval, up to a maximum of 86,400. A BES is any second that is not a UAS that contains: no LOS, AIS, or OOF conditions, and between 2 and 319 (inclusive) EEs.
SES	This field lists the number of severely errored seconds (SESs) that have occurred, up to a maximum of 86,400. An SES is any second that is not a UAS that contains: an LOS condition, or an AIS condition, or an OOF condition, or 320 or more EEs.
UAS	This field lists the number of unavailable seconds (UASs) that have occurred, up to a maximum of 86,400. A UAS state is declared when ten consecutive SESs occur. The ten SESs are subtracted from the SES count and added to the UAS count. Subsequent seconds are accrued to the UAS count until the UAS state is cleared. The UAS state is cleared when ten consecutive non-SESs occur. When that happens, the consecutive ten non-SESs are subtracted from the UAS count.
CSS	This field lists the number of controlled slip seconds (CSSs) that have occurred, up to a maximum of 86,400. A controlled slip second is any second that contains one or more controlled slips (see also the definition for ES). Note that CSSs are accumulated during unavailable seconds (UASs).

During any one-second time period, the above error events can occur in various combinations. The possible combinations are: no errors; ES; CSS; ES and CSS; ES and BES; ES and BES and CSS; ES and SES; ES and SES and CSS; UAS; UAS and CSS.

Field header	Definition
DM	This field lists the number of degraded minutes (DMs) that have occurred, up to a maximum of 1,440. A DM is a sixty non-UAS and non-SES second period that contains 49 or more CRC6 or BPV errors (ESF framing) or 49 or more bipolar violations (SF framing).
STATUS	This field shows the type of errored conditions that occurred during the time interval. The conditions are indicated by a single character as described below. In order of severity, the conditions are: **L** An LOS condition has occurred, but has not necessarily integrated to an alarm state. Inbound traffic has stopped. **O** An OOF condition has occurred, but has not necessarily integrated to an alarm state. Inbound traffic has stopped. **A** An AIS condition (but not necessarily an alarm) has occurred. Inbound traffic has stopped. **Y** A yellow alarm has been detected. Outbound traffic may have stopped. **E** An Excessive Error Rate (EER) condition (but not necessarily an alarm) has occurred. This condition can occur only if the EER alarm is enabled. Inbound traffic contains errors. **@** One of the preceding conditions has persisted long enough to cause an alarm state. **B** For both ESF and SF, a "B" is displayed if a BPV occurs. **C** If ESF is enabled, a "C" is displayed if a CRC6 error occurs. **T** There is a (loopback, code generation, or BERT) test active on the DataSMART.

[1] A controlled slip is declared when the DataSMART detects an accrued timing difference of exactly one frame between the transmitted and received data streams, resulting in the deletion or addition of a single frame in the received data stream.

Interpreting the Far-end report

*The **FESR** and **FELR** commands display the performance history of the received signal at the far-end network interface.*

Because the Far-end reports are based on PRMs, the far-end device must be T1.403 compatible. Also, PRM generation must be enabled in the near-end and far-end devices, and the T1 line's framing format must be ESF. (Use the **EPRM** command to enable PRM generation in the DataSMART and use the **NESF** command to enable ESF framing format.)

The Far-end reports show you T1 line performance as seen by the device on the far end of the circuit, without the need to connect to the far-end device directly. Using the Far-end reports and the NI statistical reports (see "Interpreting the User NI and User TI reports" on page 118) gives you a clear picture of T1 performance in both the transmit and receive directions.

The figure below shows an example of a short version of the Far-end report. Notice that it is the same as a User NI report except for the status codes described in the header and listed in the status column.

```
KENTROX DataSMART - FAR END PRM SHORT PERFORMANCE REPORT
ADDRESS: 00:00:000              NAME: PORTLAND,OR
DATE: JAN 13, 1995              TIME OF DAY: 10:53
STATUS CODES: C=CRC6, V=LCV, F=FRAME BIT ERR, E=SEVERE FRAME BIT,
              S=SLIP, P=PAYLOAD LOOP BACK, M=MISSED 4 PRM, N=NO POWER
SECOND OF INTERVAL: 495 OF 900  COMPLETED INTERVALS: 1 OF 96

                    G.821          G.821  G.821         G.821
              EE      ES    BES     SES    UAS    CSS    DM     STATUS
            ------  -----  -----  -----  -----  -----  ----  ----------
CUR SEC        319      1      1      0      0      0     0  C VF
PRE SEC        319      1      1      0      0      0     0  C VF
CUR 15-MIN    6776     59     59      0      0      0     1  C VFE  M
PRE 15-MIN       -      -      -      -      -      -     -
CUR 24-HR        -      -      -      -      -      -     -
```

What to look for and how to interpret time intervals

The items to look for in the Far-end reports and User NI reports are the same, except the Far-end reports do not include alarm states. Also, time intervals are the same in the Far-end reports and User NI reports. See page 119.

The following table describes the performance data displayed in the Far-end report.

Field header	Description
EE	This first field lists the number of error events (EEs) that have occurred, up to a maximum of 999,999. Only CRC6 errors are used to calculate error events. The PRM message does not provide exact counts of CRC6 error events. Instead it uses 6 bits that indicate that the error rate fell within a certain range; then the highest number in the range (except for the last range, as noted below) is used as the error count in the Far-end report as follows: 1 CRC6 error-per-second counts as one EE 2 to 5 CRC6 errors-per-second count as 5 EEs 6 to 10 CRC6 errors-per-second count as 10 EEs 11 to 100 CRC6 errors-per-second count as 100 EEs 101 to 319 CRC6 errors-per-second count as 319 EEs 320 or more CRC6 errors-per-second count as 333 EEs
ES	This field lists the number of errored seconds (ESs) that have occurred during the time interval, up to a maximum of 86,400. An ES is any second that is not a UAS that contains one or more CRC6 errors.
BES	This field lists the number of bursty errored seconds (BESs) that have occurred during the time interval, up to a maximum of 86,400. A BES is any second that is not a UAS that contains between 2 and 319 (inclusive) CRC6 errors.
SES	This field lists the number of severely errored seconds (SESs) that have occurred during the time interval, up to a maximum of 86,400. An SES is any second that is not a UAS that contains 320 or more CRC6 errors.
UAS	This field lists the number of unavailable seconds (UASs) that have occurred, up to a maximum of 86,400. A UAS state is declared when ten consecutive SESs occur. The ten SESs are subtracted from the SES count and added to the UAS count. Subsequent seconds are accrued to the UAS count until the UAS state is cleared. The UAS state is cleared when ten consecutive non-SESs occur. When that happens, the consecutive ten non-SESs are subtracted from the UAS count.
CSS	This field lists the number of controlled slip seconds (CSSs) that have occurred during the time interval, up to a maximum of 86,400. A controlled slip second is any second that contains one or more controlled slips (see also the definition for ES). Note that CSSs are accumulated during unavailable seconds (UASs).
During any one second time period, the above error events can occur in various combinations, which are: no errors; ES; CSS; ES and CSS; ES and BES;ES and BES and CSS; ES and SES; ES and SES and CSS; UAS; UAS and CSS.	
DM	This field lists the number of degraded minutes (DMs) that have occurred during the time interval, up to a maximum of 1,440. A degraded minute is a sixty non-UAS and non-SES second period that contains 49 or more CRC6 errors (ESF framing) or 49 or more bipolar violations (SF framing).

Field header	Description
Status	This field shows the type of errored conditions that occurred during the time interval. The conditions are indicated by a single character as described below: **F** A frame synchronization bit error has occurred in the received network signal. A frame synchronization bit error occurs when an error in the framing-bit-pattern is received. **E** A severely-errored framing event has occurred in the received network signal. A severely-errored framing event occurs when two or more framing-bit-pattern errors occur within a 3-millisecond period. **C** A CRC6 error has been detected in the received T1 signal. **V** A line code violation condition has occurred in the received network signal. A line code violation occurs when a bipolar violation that is not part of a zero-substitution code is received. **S** A controlled slip has occurred at the received network signal. A controlled slip event occurs when there is a replication or deletion of a T1 frame by the receiving network interface. **P** A payload loopback is active on the network interface. **M** No PRMs have been received for four or more consecutive seconds. Each PRM contains information for four consecutive seconds, and so no data is lost if up to three PRMs are missing.

Interpreting the Carrier NI report

The Carrier NI report allows you to view the carrier's version of the performance data of the NI signal received by the DataSMART. The carrier accesses the report from the network using the T1 facility data link. ESF framing is required.

TIP
For the purpose of monitoring the NI performance, there is generally no reason to use the Carrier NI report. The same information is available in more detail in the User NI report.

At many sites, the DataSMART is at the point of demarcation on a T1 line between a carrier and a customer premise. Therefore, the DataSMART keeps two sets of registers, both of which collect performance data on the unit's signal received at the network interface: one set of registers for the customer and one set of registers for the carrier.

The customer can view the performance data collected in the customer registers by using the User NI report. The customer can also view the performance data collected in the carrier registers by using the Carrier NI report. The carrier accesses the data in the carrier registers from a remote device using the facility data link.

The customer cannot alter the data in the contents of the carrier's registers (clear it, for instance), nor can the carrier alter the data in the customer's registers.

The format of the Carrier NI report is similar to that of the User NI report. The figure below shows a short version (using the **CNSR** command), though a long version (using the **CNLR** command) is available. The method of calculating the values in the report is per AT&T 54016.

Performance measurements are defined on page 120, except for LOFC (Loss of Frame Count). This measurement indicates two or more framing bit errors have been received within a 3-millisecond period.

```
KENTROX DataSMART - CARRIER NI SHORT PERFORMANCE REPORT
ADDRESS: 00:00:000              NAME: PORTLAND,OR
DATE: FEB 14, 1997              TIME OF DAY: 16:52
SECOND OF INTERVAL: 501 OF 900  COMPLETED INTERVALS: 2 OF 96
              EE      ES    BES    SES    UAS    CSS    LOFC
            ------  -----  -----  -----  -----  -----  -----
CUR SEC          0      0      0      0      0      0      0
PRE SEC          0      0      0      0      0      0      0
CUR 15-MIN       0     10      0      0      0     10      0
PRE 15-MIN    3692     20      2      0     10     18      0
CUR 24-HR     3694     40      2      5     25     33      2
```

Interpreting the Alarm History report

*The Alarm History report (use the **AHR** command) shows the last 20 alarm messages. The alarm messages in the report are the same messages sent to the control port device when the control port alarm messages are enabled and configured for ASCII format.*

Alarm messages are generated by physical-layer alarm states on the network interface or data port. A message is added to the report every time the network interface or data port changes to a different alarm state. The "Alarm Cleared" message is not issued unless all alarms on that line are cleared. The report logs up to twenty messages, most recent first. Once the report reaches twenty messages, new alarm messages cause the oldest message to be dropped.

See "Monitoring alarm messages" on page 133 for a full list of the types of alarm messages that can appear in this report and their meanings.

TIP
Using SMARTools Installer, this information can be printed out to disk and saved for later use.

The alarm messages are always displayed in user format (ASCII text).

Alarm messages always appear in the Alarm History report, even if alarm messages are disabled with the **DAM** command in the Alarm Configuration Menu.

Information in the Alarm History report is not cleared when an **ST**, **SD**, or **ZALL** command is executed.

The following actions clear the Alarm History report:

- Power cycling the DataSMART
- Executing the **RSD** command (see "Resetting to default values" on page 52)
- Executing the **BOOT** command (see "Obtaining new system software" on page 50)

An example of the Alarm History report is shown below.

```
SET ALM FEB.14,1997 16:37 TI EER PORTLAND,OR         addr = 01:00:000
SET ALM FEB.14,1997 16:37 NI EER PORTLAND,OR         addr = 01:00:000
SET ALM FEB.14,1997 16:36 TI LOS PORTLAND,OR         addr = 01:00:000
CLR ALM FEB.14,1997 16:32 NI     PORTLAND,OR         addr = 01:00:000
CLR ALM FEB.14,1997 16:22 TI     PORTLAND,OR         addr = 01:00:000
SET ALM FEB.14,1997 16:22 TI OOF PORTLAND,OR         addr = 01:00:000
SET ALM FEB.14,1997 16:22 TI LOS PORTLAND,OR         addr = 01:00:000
SET ALM FEB.14,1997 16:16 NI EER PORTLAND,OR         addr = 01:00:000
SET ALM FEB.14,1997 16:16 NI LOS PORTLAND,OR         addr = 01:00:000
SET ALM FEB.14,1997 16:16 NI EER PORTLAND,OR         addr = 01:00:000
CLR ALM FEB.14,1997 16:16 NI     PORTLAND,OR         addr = 01:00:000
SET ALM FEB.14,1997 16:15 NI LOS PORTLAND,OR         addr = 01:00:000
CLR ALM FEB.14,1997 16:02 NI     PORTLAND,OR         addr = 01:00:000
SET ALM FEB.14,1997 16:01 NI LOS PORTLAND,OR         addr = 01:00:000
```

Interpreting the Security History report

*The Security History report (use the **SHR** command) shows the last 10 events that might indicate unauthorized attempts to access the DataSMART.*

The report includes three types of events:

- An incorrect Telnet password has been entered (Telnet Password);
- The DataSMART has read or written an incorrect SNMP community string (SNMP Rd CommString or SNMP Wr CommString);
- The DataSMART has received an IP packet from a host whose IP address is not on the Source Screening Address list (IP Screen).

The report logs up to 10 events, most recent first. Once the report reaches 10 events, subsequent messages cause the oldest event to be dropped.

The IP address of the device which caused the security event is listed under "Comments."

You can configure the SNMP agent to send an SNMP Authentication Trap whenever one of these security events occurs. To configure these traps, see "Configuring for SNMP" on page 189.

Information in the Security History report is not cleared when an **ST**, **SD**, or **ZALL** command is executed.

The following actions clear the Security History report:

- Power cycling the DataSMART
- Executing the **RSD** command (see "Resetting to default values" on page 52)
- Executing the **BOOT** command (see "Obtaining new system software" on page 50)

An example of the Security History report is shown below.

```
Date/Time          Security Event        Comments
-----------------  --------------------  ----------------------------
FEB.13,1997 11:58  Telnet Password       Src IP Addr: 192.0.2.1
FEB.13,1997 11:52  SNMP Wr CommString    Src IP Addr: 192.0.2.1
FEB.12,1997 10:51  IP Screen             Src IP Addr: 192.0.2.11
```

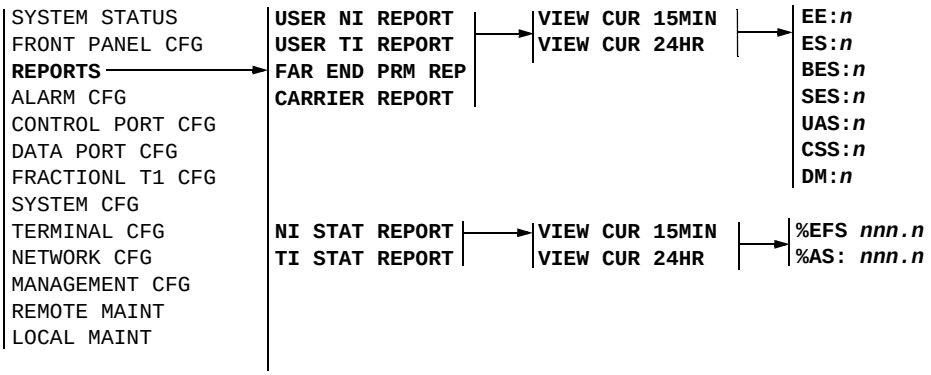
Accessing reports from the front panel

The front panel provides T1 performance reports for the network interface (user and carrier version) and the far end. It also provides a statistical version of the network interface data. The T1-layer information available from the front panel is limited to the current 15-minute interval and the current 24-hour interval.

Frame group reports and frame individual reports are also available from the front panel for the transmit and receive directions. Frame individual reports display only the information for the current 2-hour interval and the current 24-hour interval from the front panel. Frame group reports display the information for the current 15-minute interval, the current 2-hour interval and the current 24-hour interval from the front panel.

Performance reports

To view the performance reports from the front panel, use these steps.



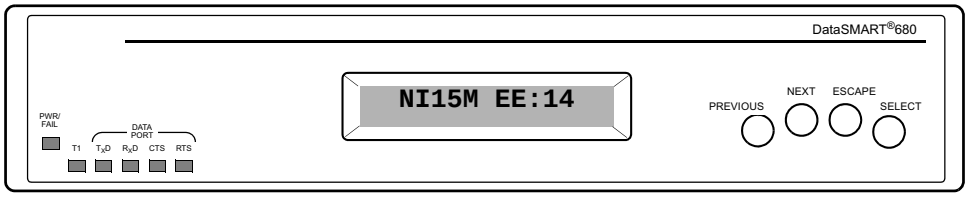
1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until REPORTS appears in the display.
3. Push Select. USER NI REPORT appears in the display.
4. Push Next or Previous until you see the desired report in the display.
5. Push Select. VIEW CUR 15MIN appears in the display.
6. Push Next or Previous to switch to VIEW CUR 24HR, if desired.
7. Push Select to view the first report display.
8. Push Next or Previous to cycle through the report displays.

Abbreviation	Term and reference page
EE	Error events. See page 120.
ES	Errored seconds. See page 120.
BES	Bursty errored seconds. See page 120.
SES	Severely errored seconds.See page 120.
UAS	Unavailable seconds. See page 120.
CSS	Controlled slip seconds. See page 120.

Abbreviation	Term and reference page
DM	Degraded minutes. See page 121.
%AS	Percent available seconds. See page 115.
%EFS	Percent error-free seconds. See page 115.

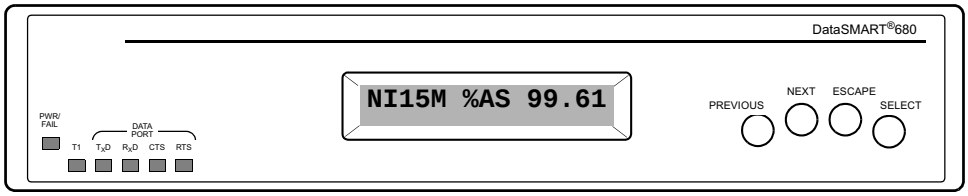
Interpreting the LCD performance display

The figure below shows a situation in which the user has selected the User NI report for the current 15-minute time slice, as indicated by "NI15M" in the display. The display is positioned at the count for error events. Pushing Next or Previous will cycle through displays to show the counts for errored seconds, bursty errored seconds, and others.



The display is dynamic. The counts in the display update as new events occur. If the display is for the current 15-minute interval, the count resets to zero when a new 15-minute interval is entered (at 00:15, 00:30, 00:45, etc.). If the report shows the current 24-hour interval, the interval is rolling and always shows the totalled count for the previous ninety-six 15-minute intervals.

The display for the statistical information is similar to the performance reports. For example, the figure below shows the User NI report's percentage of available seconds for the current 15-minute time slice.



Clearing the performance database

At any time, you can clear the performance data and reset counters by executing the **ZERO COUNTERS** command under the **SYSTEM CFG** menu (see "Zeroing all counters" on page 49). This clears the data from all reports except the Alarm History, Security History, and Carrier NI Data reports.

Performance data is also cleared whenever you reset the date or time on the DataSMART using the **SET DATE** or **SET TIME** commands under the **SYSTEM CFG** menu (see "Setting date and time" on page 38).

C H A P T E R

7 Troubleshooting

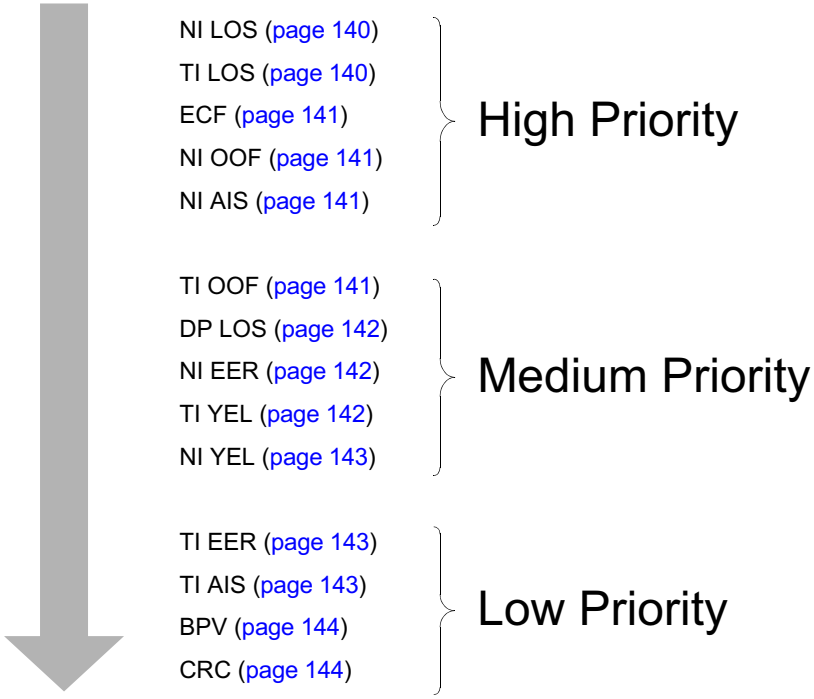
This chapter describes how to troubleshoot the DataSMART. It contains:

- How LEDs and alarm messages alert you when something is wrong
- How to find out the type of alarm and the interface at which it is occurring using either the front-panel or the command-line interface
- A list of all error conditions in the System Status report and suggestions of how to resolve them
- A description of how to use the DataSMART diagnostic tools, including self test, loopbacks, and BERTs

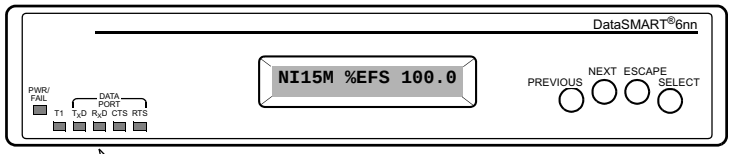
Following is a quick guide to the alarms generated by the DataSMART and to the pages in this chapter that provide appropriate troubleshooting procedures for the alarms. The alarms are prioritized high to low.

TIP
Always deal with the highest-priority alarms first.

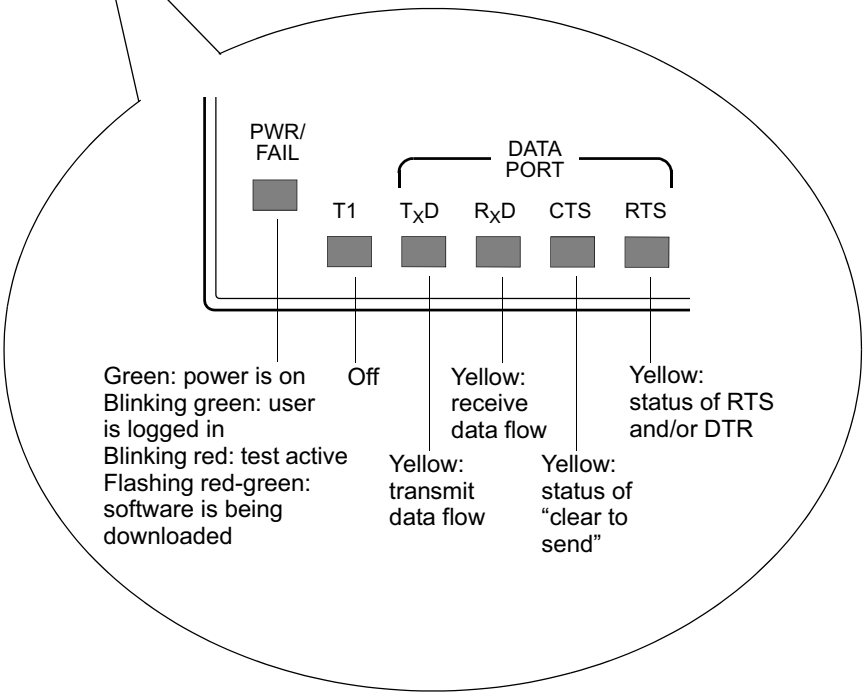
Figure 13—Troubleshooting the DataSMART



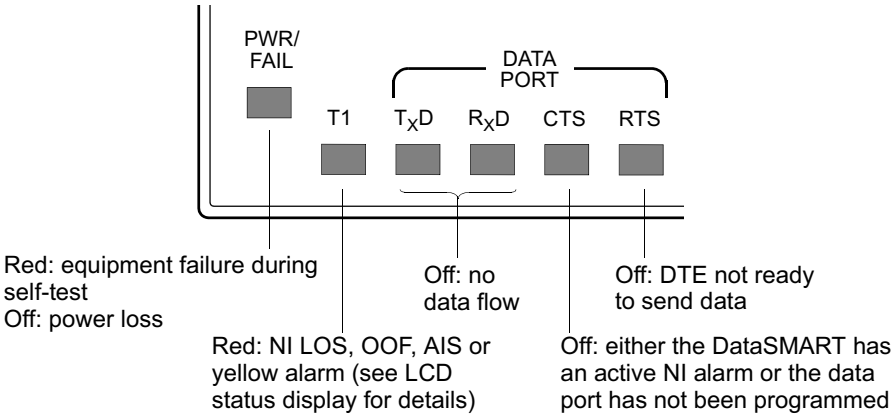
Interpreting the front-panel LEDs



NORMAL



ABNORMAL



Monitoring alarm messages

Table 5—LED indicators and their meanings

LED	Indicator	Condition
PWR/FAIL	Green	Power is on, self-test successful.
	Green, blinking	A user is logged into the DataSMART.
	Red-to-green, flashing	Software program is being downloaded.
	Blinking red	A test is active.
	Red	Power is on, self-test failed.
	Off	No power is being received.
T1	Red	One or more of the following has occurred on the network interface or terminal interface or both (see LCD status display): ■ LOS alarm. The T1 signal has been lost. ■ OOF alarm. The T1 signal is out-of-frame. Some or all of the DS1 framing bits have been lost. ■ Incoming AIS alarm. The far-end equipment (NAIS) or CPE (TAIS) is in test or alarm state. ■ Yellow alarm. The far-end equipment (NYEL) or CPE (TYEL) is experiencing LOS or OOF.
TxD	Yellow	Data is being transmitted (input) at the data port. Note that under normal conditions this LED may fluctuate in intensity.
	Extended “off”	Zeroes are being received at the data port. Zeroes are transmitted to the network if RTS and CTS are high.
RxD	Yellow	Data is being received (output) at the data port. Note that under normal conditions this LED may fluctuate in intensity.
	Off	Zeroes are being output at the data port if RTS and CTS are on.
CTS	Yellow	Channels are assigned, and NI is not in alarm. The DataSMART is ready to exchange data with the DTE.
	Off	This LED is off when it is not possible to transmit data out the data port. This may be because an NI alarm is present or the data port is not programmed or no channel is assigned.
RTS	Yellow	Request to send is asserted. The DTE is ready to send data to the DataSMART, according to the conditions established by the **DPLOS** command.
	Off	The DTE is not ready to send data (per the conditions configured by the **DPLOS** command) or is not connected or channels are not assigned.

The DataSMART generates the alarm messages listed in Table 6 and outputs them at the control port. If you receive an alarm message, you should use the Status (**S**) command to get the details of the problem.

Terminal interface alarms are generated only by add/drop units.

Only one alarm can be active at a time per unit. If two alarm conditions exist on a unit, that unit issues an alarm message only for the higher priority alarm. When the higher priority alarm is cleared, the unit then issues the next lower priority alarm, if one is still present.

Table 6—Alarms generated by DataSMART units

Alarm	Description
ECF	External clock failure. This occurs when you specify data port timing and the DataSMART cannot detect a signal on the data port external clock pins.
NI LOS	Loss of T1 signal at the network interface.
NI AIS	Incoming AIS (alarm indicator signal) at the network interface. Some device upstream of the network interface is in a LOS or OOF alarm state on the far side or in a test mode.
NI OOF	Out-of-frame T1 signal at the network interface. Some or all DS1 framing bits have been lost.
NI YEL	Incoming yellow alarm at the network interface. A device upstream of the network interface is in an OOF or LOS alarm state on the near side.
NI EER	Excessive error rate detected on the T1 signal at the network interface.
TI LOS	Loss of T1 signal at the terminal interface.
TI AIS	Incoming AIS (alarm indicator signal) at the terminal interface. Some device upstream of the terminal interface is in a LOS or OOF alarm state on the far side.
TI OOF	Out-of-frame T1 signal at the terminal interface. Some or all DS1 framing bits have been lost.
TI YEL	Incoming yellow alarm at the terminal interface. A device upstream of the terminal interface is in an OOF or LOS alarm state on the near side.
TI EER	Excessive error rate detected on the T1 signal at the terminal interface.
DP LOS	Loss of DTR and/or RTS at the data port.

Examining system status

If the DataSMART is in an alarm state or if you notice an abnormal condition, use the System Status report display to get more information. You can view the system status from the front-panel or the command-line interface. Both the front-panel display and the command-line report use the same status codes, which are explained in Table 7 on page 136.

Terminal interface alarms are generated only by add/drop units.

TIP
For a discussion of how the DataSMART transitions in and out of alarm states based on errored signal conditions, see "T1 alarms and signal processing" on page 214.

The system status tells you the current condition of the DataSMART, including any alarms that may be active as well as current — and possibly intermittent— signal conditions at the network interface, the terminal interface, and the data ports. Both the LCD status display and the command-line status display are dynamic and are updated as conditions change on the DataSMART.

Using the command line

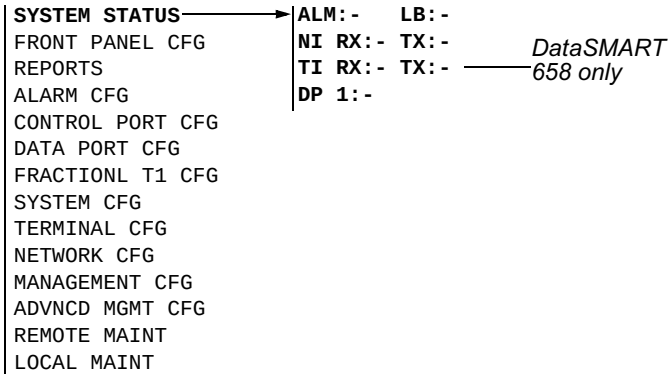
To see the command-line display, enter **S** at the prompt. A screen similar to the one shown below appears. The display is updated once per second if the status changes, with the new status line added at the bottom. You exit the display by pressing Ctrl-C.

```
OPERATIONAL STATUS (^C TO EXIT)

JAN  4, 1997

TIME   SYSTEM     NI       TI       Data Port
-----  ---------  -------  -------  ---------
       ALRM LPBK  IN  OUT  IN  OUT  DP1
-----  ---- ----  --- ---  --- ---  ---
07:31  NLOS -     LOS YEL  LOS AIS  CON
```

Screen column	Description
TIME	This column shows the time of day (in 24-hour format) that the status line was generated.
SYSTEM ALRM	This column shows the highest priority state.
SYSTEM LPBK	This column shows if a loopback is active.
NI IN, NI OUT	These columns show the network interface RCV and XMT signal conditions.
TI IN, TI OUT	These columns show the terminal interface RCV and XMT signal condition (add/drop units only).
Data Port	These columns show the data port input signal condition.

Using the front panel

To view system status from the front panel, use these steps.



1 Push Escape until SYSTEM STATUS appears in the display.

2 Push Select to see the first system status display.

3 Push Next or Previous to cycle through the other status displays.

Status codes

Table 7 explains the status codes and refers to a page for possible solutions.

Table 7—Status codes

Code	Description	Solution
ALRM — Alarm Status		
—	No alarm exists.	Normal behavior.
ECF	External clock failure.	See page 141
NLOS	Loss of the network input signal.	See page 140
NOOF	The network input signal is out of frame.	See page 141
NAIS	Incoming AIS (alarm indication signal) at the network interface.	See page 141
NYEL	Incoming yellow alarm at the network interface.	See page 143
NEER	Excessive error rate detected on the network input signal.	See page 142
TLOS	Loss of the terminal input signal.	See page 140
TOOF	The terminal input signal is out of frame.	See page 141
TAIS	Incoming AIS (alarm indication signal) at the terminal interface.	See page 143
TYEL	Incoming yellow alarm at the terminal interface.	See page 142
TEER	Excessive error rate detected on the terminal input signal.	See page 143
1LOS	Loss of DTR and/or RTS at data port 1.	See page 142

Table 7—Status codes (continued)

Code	Description	Solution
LPBK — Loopback Status		
—	No loopback is set.	Normal behavior.
RLLB	Code has been sent to set a remote line loopback.	Loopback test in progress.
RPLB	Code has been sent to set a remote payload loopback.	Loopback test in progress.
RDP1	Code has been sent to set remote data port loopback.	Loopback test in progress.
LLB	A line loopback is set on the local device.	Loopback test in progress.
LOC	A local loopback is set on the local device.	Loopback test in progress.
PLB	A payload loopback is set on the local device.	Loopback test in progress.
TLB	A terminal loopback is set on the local device.	Loopback test in progress.
DP1	A data port loopback is set on the local device.	Loopback test in progress.
DT1	A data terminal loopback is set on the local device.	Loopback test in progress.
NI IN (Rx) — Network Input Status		
LOS	Loss of the network input signal.	See page 140
OOF	The network input signal is out of frame.	See page 141
AIS	Incoming AIS (alarm indication signal) at the network interface.	See page 141
YEL	Incoming yellow alarm at the network interface.	See page 143
BPV	A bipolar violation has been detected on the network input signal. This applies only if the network signal is using SF framing.	See page 144
CRC	A cyclic redundancy check error has been detected on the network input signal. Seen only if the network signal is using ESF framing.	See page 144
QRS	A BERT running QRS test code is active at the network interface.	Normal behavior when a BERT is active.
324	A BERT running 3 in 24 test code is active at the network interface.	Normal behavior when a BERT is active.
247	A BERT running 2047 test code is active at the network interface.	Normal behavior when a BERT is active.
511	A BERT running 511 test code is active at the network interface.	Normal behavior when a BERT is active.
1’S	A BERT running all 1s test code is active the network interface.	Normal behavior when a BERT is active.
0’S	A BERT running all 0s test code is active at the network interface.	Normal behavior when a BERT is active.
—	Valid data is being received. No errors detected.	Normal behavior.

Table 7—Status codes (continued)

Code	Description	Solution
NI OUT (Tx) — Network Output Status		
AIS	AIS (alarm indication signal) is being transmitted out the network interface.	See page 141
YEL	Yellow alarm is being transmitted out the network interface. This occurs when LOS, OOF, or incoming AIS is detected at the network input signal.	See the entry in this table for Network input status codes LOS, OOF, or AIS.
QRS	QRS test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
324	3 in 24 test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
247	2047 test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
511	511 test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
1'S	All 1s test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
0'S	All 0s test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
COD	The DataSMART is in the process of setting or resetting a remote loopback.	Normal behavior.
—	Valid data is being transmitted out the network interface.	Normal behavior.
TI IN (Rx) — Terminal Input Status (658 only)		
LOS	Loss of the terminal input signal.	See page 140
OOF	The terminal input signal is out of frame.	See page 141
AIS	Incoming AIS (alarm indication signal) at the terminal interface.	See page 143
YEL	Incoming yellow alarm at the terminal interface.	See page 142
BPV	A bipolar violation has been detected on the terminal input signal.	See page 144
CRC	A cyclic redundancy check error has been detected on the terminal input signal. Seen only if the terminal signal is using ESF framing.	See page 144
—	Valid data is being received. No errors detected.	Normal behavior.
TI OUT (Tx) — Terminal Output Status (658 only)		
YEL	Yellow alarm is being transmitted out the terminal interface. This occurs when incoming yellow alarm is detected at the network input signal.	Troubleshoot the alarm causing the output.
AIS	AIS (alarm indication signal) is being transmitted out the terminal interface. This occurs when LOS, OOF or incoming AIS is detected on the network input signal.	Troubleshoot the alarm causing the output.

Table 7—Status codes (continued)

Code	Description	Solution
—	Valid data is being transmitted out the terminal interface.	Normal behavior.
Data Port (DP)		
—	No bandwidth (channels) have been assigned to the data port.	Normal behavior.
CON	Bandwidth is assigned to the port, and the port is not in a LOS condition.	Normal behavior.
LOS	Bandwidth is assigned to the port, but a loss of DTR or RTS has been detected.	See page 142

Troubleshooting tree

Troubleshooting alarms

The best troubleshooting method is to start with the highest priority alarm, find its cause and fix it, and then turn to the next highest priority. The following alarm list is arranged from high to low priority. You may also want to use some of the diagnostic tools described later in this chapter.

NOTE

In this manual, high-priority alarms tend to arise from more basic problems than low-priority alarms. Often, fixing a high-priority alarm will also automatically correct alarms of lower priority. Network management systems use the words "critical," "major," and "minor" to rank alarms in terms of seriousness. These two rankings are similar, but not always identical.

NI LOS—high priority

If you receive a loss-of-signal condition at the network interface...

An NI LOS condition occurs when the DataSMART cannot detect a signal at its network interface. To troubleshoot for this condition:

- Make sure that you have correctly connected the cable between the DataSMART network interface and your T1 service provider's equipment.
- If you built the cable on-site, check the cable connectors. A reversal of the transmit and receive pairs, or an open receive pair, can cause this condition.
- If the above appear to be okay, ask your T1 service provider to test your T1 line and correct any problems found.

TI LOS—high priority

If you receive a loss-of-signal condition at the terminal interface...

A TI LOS condition occurs when the DataSMART cannot detect a signal at its terminal interface. To troubleshoot for this condition:

- Make sure that you have correctly connected the cable between the DataSMART terminal interface/data port and your CPE equipment.
- If you built the cable on-site, recheck the cable connectors. A reversal of the transmit and receive pairs, or an open transmit pair (CPE-to-DataSMART), can cause this condition.

NOTE

If you assign channels to the terminal interface but do not connect equipment to it, the unit will generate the TI LOS alarm.

ECF—high priority

If you receive an external clock failure (ECF) alarm...

An ECF alarm occurs when the DataSMART is configured for data port timing, but it cannot detect a clock signal at the data port, either because the signal is not present or because the signal is significantly out of timing. To troubleshoot this condition:

- Verify whether or not the DataSMART should really be set to data port timing. You should only use this timing option if a timing source is *not* provided by the T1 service. Controlled slips may occur if you set the DataSMART to data port timing when a network clock is present.
- Check the cable connection between the data port and your external clock source.
- Verify that your external clock source is powered up and configured correctly.
- Verify that your external clock source provides the correct type of clock signal, as shown in the DataSMART specifications (see Chapter 9).

NI OOF—high priority

If the incoming signal at the network interface is out-of-frame...

An out-of-frame condition occurs when the framing type you have configured for the network interface does not match the framing type of the incoming T1 signal. Allowed framing types are ESF, SF, or Ericsson. To troubleshoot this condition:

- Change the framing type of the network interface (see "Specifying NI framing format" on page 72), or
- Ask your T1 service provider to change the framing type of your T1 line.

A highly errored incoming signal can also cause an OOF condition.

NI AIS—high priority

If an alarm indication signal (AIS) is detected at the network interface...

An incoming AIS at the network interface indicates a problem with remote equipment on the T1 circuit. For example, the far-end equipment may not be connected or configured properly or is in a test mode, or the network interface unit (i.e., NIU or smart jack) may be in loopback, or your service provider may not have enabled your circuit yet. To troubleshoot this condition:

- Ask your T1 service provider to trace the source of the AIS signal.

TI OOF—medium priority

If the incoming signal at the terminal interface is out-of-frame...

An out-of-frame condition occurs when the framing type you have configured for the terminal interface does not match the framing type of the signal being received at the terminal interface. Allowed framing types are ESF, SF, or Ericsson. To troubleshoot this condition:

- Change the framing type of the terminal interface (see "Specifying TI framing format" on page 82) or
- Change the framing type of the attached CPE equipment.

Note that a highly errored incoming signal can also cause an OOF condition. Check the description of TI EER.

DP LOS—medium priority

If you receive a loss-of-signal indication at the data port...

A DP LOS condition occurs when the DataSMART is not able to handshake as expected with an attached DTE device.

The DataSMART can monitor two handshake lines on each data port: DTR and RTS. You can configure your DataSMART to use either, or both lines as the DP LOS criteria (see "Setting up DPLOS (data port loss of signal) processing" on page 94). When the specified line goes low, the DataSMART assumes that the DTE equipment has been disconnected or has failed. To troubleshoot this condition:

- Check the cable connection between the DataSMART data port and the DTE.
- Verify that the cable is connected to the correct port at each end.
- Verify that you are using the correct cable for your application.
- Make sure that the DTE is powered up and that its serial port is activated.

Refer to the *DataSMART 600 Series Installation Guide* for instructions on how to properly connect cables.

NI EER—medium priority

If an excessive error rate is detected at the network interface...

The errors may be BPVs, CRC6 errors, or framing errors. There are several potential causes of an excessive error rate at the network interface. To troubleshoot this condition:

- Make sure you haven't set too low a threshold for detecting errored seconds or unavailable seconds. A low setting increases error sensitivity. You might want to use the factory default threshold setting (see page 64).
- Make sure that you have correctly connected the cable between the DataSMART network interface and your T1 service provider's equipment. (Refer to the *DataSMART 600 Series Installation Guide* for instructions on how to properly connect the cable.)
- If you built the cable on-site, recheck the cable connectors. Loose or intermittent connections can cause an excessive error condition.
- Make sure that you have configured the line coding of the network interface to match the line coding of your T1 line: either AMI or B8ZS. (See "Specifying NI line coding" on page 73.)
- Make sure the system clock is configured correctly.
- If all the above appear to be okay, ask your T1 service provider to test your T1 line and correct any problems found.

TI YEL—medium priority

If incoming yellow alarm is detected at the terminal interface...

An incoming yellow alarm at the terminal interface indicates that the CPE equipment attached to the interface is having a problem with the signal it is receiving from the DataSMART. Most often, it is getting no signal at all. To troubleshoot this condition:

- Check for an open, short, or wiring error in the cable between the DataSMART terminal interface port and the CPE equipment. An open receive pair (DataSMART TI port output to CPE input) can cause this condition.

NI YEL—medium priority

If incoming yellow is detected at the network interface...

An incoming yellow condition at the network interface indicates that the far end equipment has a problem with the signal it is receiving from the DataSMART. To troubleshoot this condition:

- Check for an open, short, or wiring error in the cable between the DataSMART network interface port and your T1 service provider's network interface unit (i.e., NIU or smart jack). An open transmit pair can cause this condition.
- If your application uses SF framing, and all 24 channels are used for data transmission, the actual data content can sometimes cause a "false yellow" condition. ESF framing is recommended for such applications. Other work-arounds may also be possible, depending upon your application.

TI EER—low priority

If an excessive error rate is detected at the terminal interface...

The errors may be BPVs, CRC6 errors, or framing errors. There are several potential causes of an excessive error rate at the terminal interface. To troubleshoot this condition:

- Make sure you haven't set too low a threshold for detecting errored seconds or unavailable seconds. A low setting increases error sensitivity. You might want to use the factory default threshold setting.
- Make sure that you have correctly connected the cable between the DataSMART terminal interface/data port and your CPE equipment. (Refer to *DataSMART 600 Series Installation Guide* for instructions on how to properly connect the cable.)
- If you built the cable on-site, recheck the cable connectors. Loose or intermittent connections can cause an excessive error condition.
- Make sure that you have configured the line coding of the terminal interface to match the line coding of your CPE equipment: either AMI or B8ZS. (See "Specifying TI line coding" on page 83.)
- Make sure the system clock is configured correctly.

TI AIS—low priority

If an alarm indication signal (AIS) is detected at the terminal interface...

An incoming AIS at the terminal interface may indicate that the CPE equipment attached to the terminal interface is not operational. To troubleshoot this condition:

- Check the programming of the CPE and make sure that its TI port is enabled.
- Check the wiring between the DataSMART TI port and the CPE.
- Make sure that the framing type of the CPE matches the framing type configured for the terminal interface. Allowed framing types are ESF, SF, and Ericsson. (See "Specifying TI framing format" on page 82.)

BPV—low priority

If bipolar violations (BPVs) are detected at the network interface or the terminal interface...

A bipolar violation is an error in the normal polarity of received pulses. A bipolar violation occurs when two or more pulses of the same polarity appear in a row.

Bipolar violations are often caused by local problems with your T1 line. To troubleshoot this condition:

- Make sure that your T1 wiring consists of only *individually-shielded* twisted pairs.
- Check that all cable connections are secure and connected to the correct terminals. Refer to the *DataSMART 600 Series Installation Guide* for instructions on how to properly connect cables.
- Make sure that you've set the line coding of the network interface to match the line coding of the T1 circuit: either AMI or B8ZS. A mismatch in line coding can often result in BPV errors.
- Make sure the system clock is configured correctly.

CRC—low priority

If CRC6 (6-bit cyclic redundancy check) errors are detected at the network interface or the terminal interface...

CRC6 errors relate to ESF framing only. A CRC6 error indicates that bits were received in error in the previous extended superframe.

CRC6 errors are often caused by remote problems with your T1 line. To troubleshoot these types of errors:

- Make sure that you've set the line coding of the network interface to match the line coding of the T1 circuit: either AMI or B8ZS. This line code should be maintained throughout the connected circuit. A mismatch in line coding can often result in CRC6 errors.
- If the errors show up on the NI port, ask your T1 service provider to monitor the receive side of your line for CRC6 errors.
- Make sure the system clock is configured correctly.

Running the self-test diagnostics

At any time, you can initiate the DataSMART self-test. The self-test verifies the functions of DataSMART hardware circuitry. There will be a brief service interruption during the self-test.

When you execute the self-test, the DataSMART automatically resets any loopbacks and deactivates any test code generation and bit error rate tests (BERTs). It does not clear the performance database, nor does it log you out of the system.

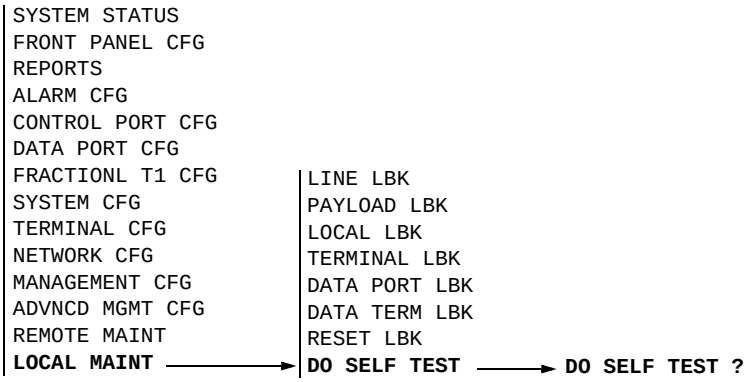
You cannot activate the self-test if you have logged into the DataSMART remotely, either through the **ARC** command or via Telnet or SNMP. The self-test would break your remote login connection.

Using the command line

To initiate self-test from the command line, enter the **DST** command. You must have super-user, configuration, or maintenance privileges.

Using the front panel

To initiate self-test from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until LOCAL MAINT appears in the display.
3. Push Select. LINE LBK appears in the display.
4. Push Next or Previous until DO SELF TEST appears in the display.
5. Push Select. The unit asks, “DO SELF TEST?”
6. Push Select to start the self test or Escape to abort.

Self-test error messages

The following messages announce pass or fail conditions discovered by the self-test. Contact our Technical Support organization if the self-test returns a “fail” condition.

Command-line display
SELF TEST PASSED
UNABLE TO PERFORM SELF TEST
FLASH TYPE FAIL
FLASH BANK 0 PROGRAM WORD FAIL
FLASH BANK 1 PROGRAM WORD FAIL
FLASH BANK 0 PROGRAM CHECK SUM FAIL
FLASH BANK 1 PROGRAM CHECK SUM FAIL
RAM PATTERN TEST FAILED
RAM CHECK SUM FAILED
RAM TEST FAILED AT ADDR:<*hex address*>
RTC TEST FAILED
NI TEST FAILED
TI READ/WRITE TEST FAILED
CGD DETECTION TEST FAILED
CGD BIT ERROR RATE TEST FAILED
DATA PORT 1 TEST FAILED

Front-panel display
SELF TEST PASSED
UNABLE TO TEST
FLASH TYPE FAIL
FLASH 0 FAIL
FLASH 0 SUM FAIL
FLASH 1 FAIL
FLASH 1 SUM FAIL
RAM PATRN FAILED
RAM CSUM FAILED
RAM ERR <*hex address*>
RTC TEST FAILED
NI R/W TEST FAIL
TI R/W TEST FAIL
CGD DETECT FAIL
CGD DATA FAIL
TSA/DP 1 FAIL

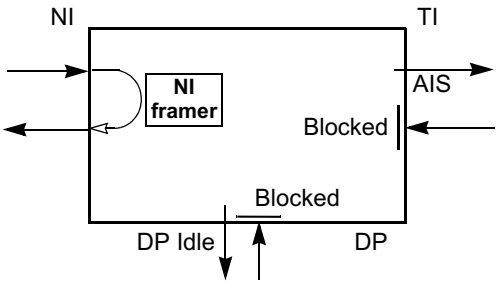
Using loopbacks

The DataSMART provides loopbacks to support line segment testing. Line segment testing allows you to probe the T1 circuit to isolate where data flow is being corrupted or disrupted.

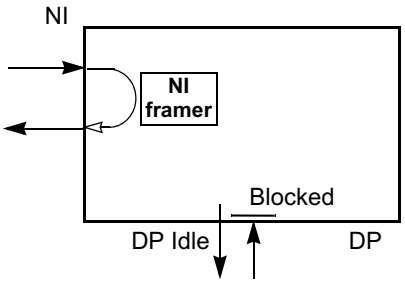
You can set all loopbacks locally, in your near-end device. You can also set the line, payload, and data port loopbacks remotely, in a far-end device. If you set a loopback in a far-end device, you can use the DataSMART to run bit error rate tests (BERTs) to test the T1 signal.

Line loopback

Add/drop



DSU



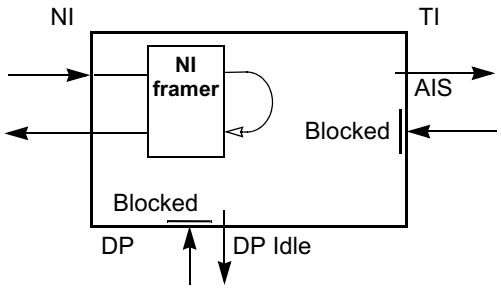
The line loopback allows the carrier (or a far-end device) to test the T1 signal at the DataSMART network interface. When set to line loopback, the DataSMART loops the incoming T1 signal back to the network. The T1 signal does not penetrate the DataSMART (it is a minimum-penetration loopback), and does not pass through the DataSMART framer. The signal, including framing and line coding errors, is returned to the network unaltered and the carrier can test the looped signal for errors.

Once the line loopback is set, the incoming network signal is interrupted, so the DataSMART outputs AIS at the terminal interface and idle characters at the data port.

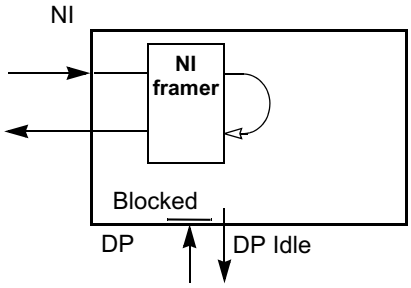
You can set the line loopback locally using the command line or front panel (see page 154); or remotely in a far-end device (see page 156).

Payload loopback

Add/Drop



DSU



TIP
You can also use a bi-directional BERT to isolate T1 line problems. See page 158.

By testing the T1 signal through a line loopback as described earlier, the carrier (or the far-end device) can determine if there are problems in the network line. What they cannot determine, however, is whether the problems are occurring on the input or output side of the looped line. To further isolate the source of the problems to one side of the line or the other, you can change from a line loopback to a payload loopback.

Payload loopback is the same as line loopback, except that the signal passes through the DataSMART framer before being looped back. The framer strips out BPV errors and recalculates CRC (for ESF framing format) but does not alter the payload data.

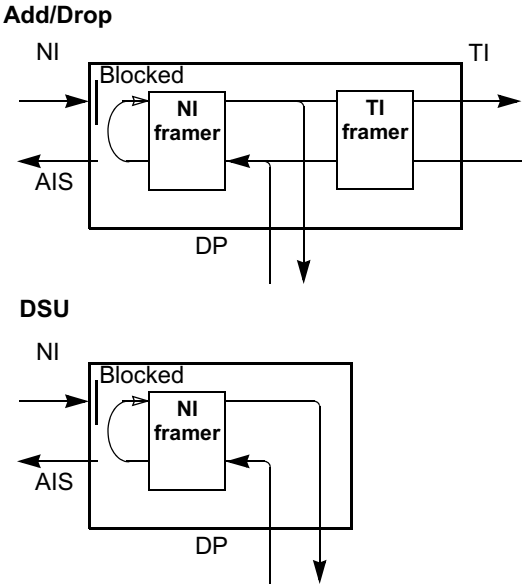
The condition of the returned signal indicates the cause of the problem:

- The line is okay if the returned signal contains no bit pattern errors, no BPVs, and no CRC6 errors.
- The problem is outbound if the returned signal contains pattern bit errors, but no BPVs or CRC6 errors.
- The problem is inbound and at the remote end if the returned signal contains pattern bit errors and CRC6 errors, but no BPVs.
- The problem is inbound and at the local end if the returned signal contains pattern bit errors, CRC6 errors, and BPVs.
- The problem is probably a remote clock slip if the returned signal contains pattern bit errors and is bursty, but contains no BPVs and no CRC6 errors.

Once the payload loopback is set, the incoming network signal is interrupted, and so the DataSMART outputs idle characters at the data ports and AIS at the terminal interface.

You can set the payload loopback locally at the request of the carrier or a far-end site (see page 154), or you can set it remotely in a far-end device (see page 156).

Local loopback



TIP
The local loopback is similar to a "hard" loopback set at the network interface.

Add/Drop units

The local loopback allows you to verify if the DataSMART is assigning channels correctly to the terminal interface and data port. When set in this loopback, the DataSMART combines all the incoming channels from the terminal interface and data port into the T1 bit stream, runs the bit stream through the NI framer, loops the bit stream back, and drops out the channels to the data port and/or terminal interface. By attaching terminal devices capable of monitoring the looped signals, you can verify that the correct channels are being returned to the correct ports.

DSUs without terminal interface

The local loopback allows you to test transmission from the DTE to the data port. This loopback combines all the incoming channels from the data port into the T1 bit stream, runs the bit stream through the NI framer, loops the bit stream back, and returns the assigned channels to the data port. By attaching a DTE device capable of monitoring the looped signal, you can verify the quality of the returned signal.

All units

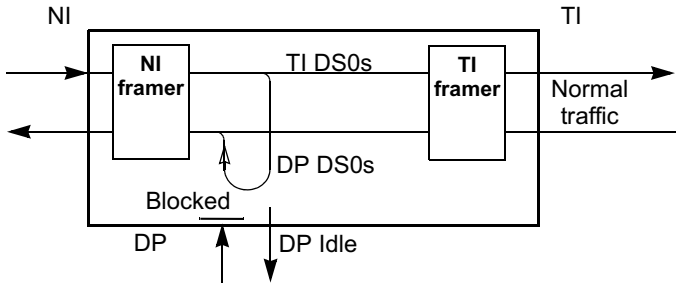
When the DataSMART is set in a local loopback, the outgoing T1 signal at the network interface is interrupted. The DataSMART outputs AIS at the network interface.

The framer strips out BPV errors and recalculates CRC (for ESF framing format) but does not alter the payload data.

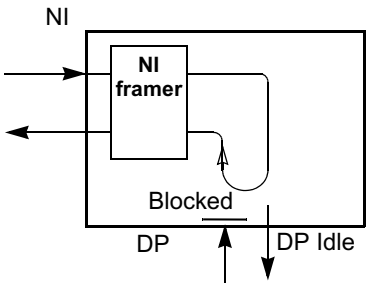
You can only set a local loopback in your local DataSMART (see page 154); you cannot set it remotely.

Data port loopback

Add/Drop



DSU



The data port loopback allows the carrier (or a far-end device) to examine the fractional DS0 channels assigned to the data port. When set to data port loopback, the DataSMART receives the T1 signal at the network interface, distributes the fractional DS0 channels as assigned to the data port, then loops the channels back to the network. It does this without affecting the rest of the received payload. Normal transmission occurs at the terminal interface.

Add/Drop units

Full-bandwidth test codes (QRSS, 3 in 24, all-1s, all-0s) will fail if the unit has some network interface channels set to the terminal interface and others set to the data port because of differences in timing delays between the terminal interface and data port circuits. You can remedy this problem by doing one of the following during the test:

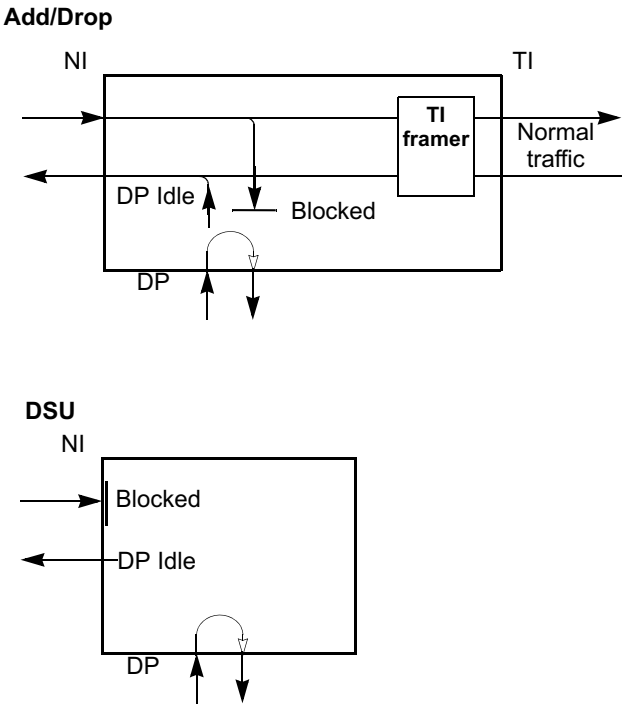
- Assign all channels to the terminal interface.
- Assign all channels to the data port (rate=64 Kbps per channel).
- Use a different test pattern.

All units

Once the data port loopback is set, transmission at the data port is interrupted. The DataSMART sends idle characters out the port to notify the connected DTE device.

You can set the data port loopback locally to facilitate testing with the carrier or a far-end site (see page 154), or you can set it remotely in a far-end device (see page 156).

Data terminal loopback



Typically, you use the data terminal loopback to verify the cabling between the data port and the attached DTE device. You can also monitor the looped signal for errors at the DTE.

The data terminal loopback allows you to loop the incoming signal at the data port. When set in this loopback, the DataSMART loops the incoming signal back to the DTE device sending the signal. The signal does not penetrate the DataSMART. The signal, including all line coding errors, is returned to the DTE device unaltered.

You can only set a data terminal loopback in your local DataSMART (see page 154); you cannot set it remotely.

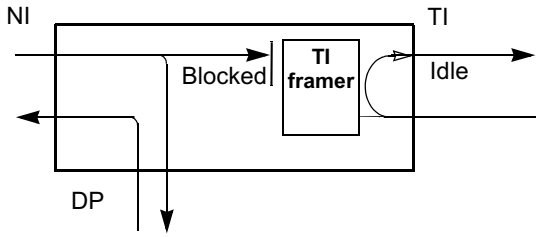
Add/drop units

When set in a data terminal loopback, the DataSMART inserts the data port idle character into the channels assigned to the data port. Normal activity continues at the network interface and the terminal interface.

DSUs without terminal interface

When set in a data terminal loopback, the DataSMART outputs AIS or a framed all-ones signal at the network interface (see “Specify the “keep alive” signal for the network interface (add/drop units only)” on page 78).

Terminal interface loopback (Add/Drop units only)



Typically, you use the terminal interface loopback to verify the cabling between the terminal interface and the CPE. You can also attach a test set to the terminal interface, send test codes, then run bit error rate tests on the looped signal.

The terminal interface loopback allows you to loop the incoming T1 signal at the terminal interface in add/drop devices. When set in this loopback, the DataSMART loops the incoming T1 signal back to the CPE attached to the terminal interface. The signal does not penetrate the DataSMART. The signal, including all line coding errors, is returned to the CPE unaltered.

When set in a terminal interface loopback, the DataSMART inserts the TI idle character into channels assigned to the terminal interface. Normal activity continues at the network interface and data port.

You can only set a terminal interface loopback in your local DataSMART (see page 154); you cannot set it in a remote device.

Setting and resetting loopbacks in your local device

You can set and reset loopbacks in your local device from the command line. Only one loopback, either local or remote, may be set at one time. You cannot set a loopback if another loopback is already active, if test codes are being transmitted, or if a BERT is active.

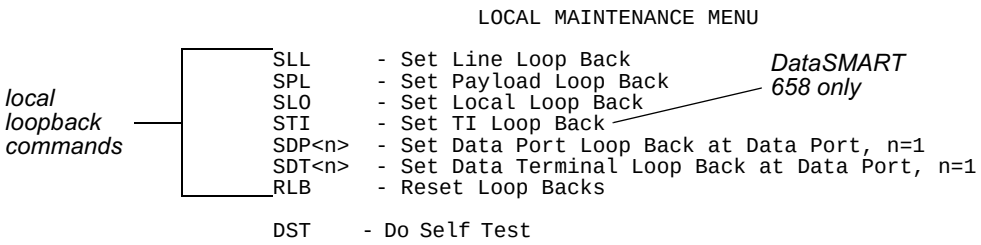
If you have logged into the DataSMART via the **ARC** command, the DataSMART *does not* allow you to set any loopback because loopbacks can potentially break the data link. The DataSMART *does* allow you to set the line, payload, and data port loopbacks via Telnet or SNMP. However, if you are managing the DataSMART via the T1 payload (using the FDL or a DS0 channel as a data link), be aware that these loopbacks could potentially break the connection by breaking the T1 payload.

NOTE

A far-end device can set your local device in line, payload, or data port loopback by sending the remote loopback commands described in the next section. A far-end device can also set your device in line loopback by sending standard line loopback set and reset code, or in data port loopback by sending 127 set code and inverted 127 reset code (V.54 loop code).

Using the command line

The figure below illustrates the Local Maintenance menu. You use the commands in this menu to set or reset loopbacks in your local device. You must have super-user, configuration, or maintenance privileges.

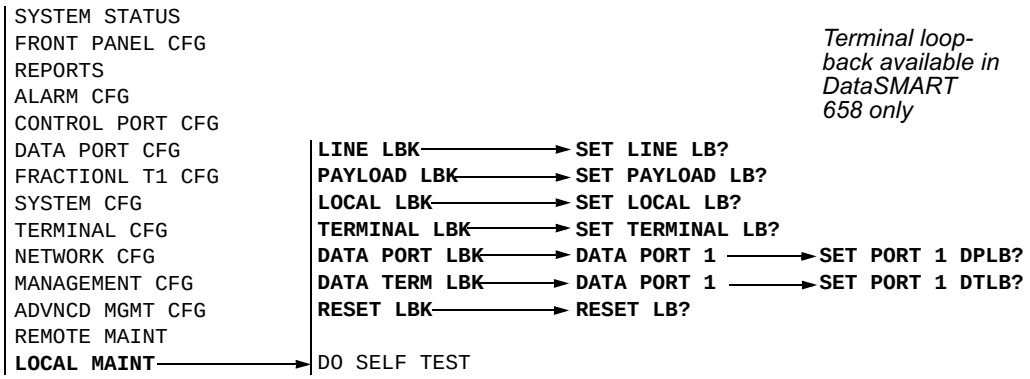


SLL	Set a line loopback.
SPL	Set a payload loopback.
SLO	Set a local loopback.
STI	Set a terminal interface loopback (in add/drop units only).
SDP1	Set a data port loopback on data port 1.
SDT1	Set a data terminal loopback on data port 1.

To reset a loopback in your local DataSMART, enter **RLB**.

Using the front panel

To set or reset local loopbacks from the front panel, use these steps. You must have super-user, configuration, or maintenance privileges.



1 Push Escape until SYSTEM STATUS appears in the display.

2 Push Next or Previous until LOCAL MAINT appears in the display.

3 Push Select. LINE LBK appears in the display.

4 Push Next or Previous until the desired command appears in the display. Note that the RESET LBK command is only available if a loopback has already been set.

5 Push Select. If you select either the data port loopback or the data terminal loopback, you must select the desired data port. Push Next or Previous until the desired data port appears in the display and push Select.

6 A query asks if you really want to set or reset the loopback. Push Select to set the loopback. LOOPBACK SET appears in the display.

7 After a few seconds, the message RESET LBK appears ("resetting" the loopback turns it off). When you are ready to turn the loopback off, push Select. A query asks if you really want to reset the loopback; push Select to turn off the loopback.

Setting and resetting loopbacks remotely

You can set a line, payload, or data port loopback remotely, in a far-end device. If you set one of these loopbacks, you can then send a test code through the loop and run BERTs on the code to troubleshoot for errors. This section describes how to set and reset remote loopbacks. For a description of how to set and run test codes and BERTs, see page 158.

Only one loopback, either local or remote, may be set at one time. You cannot set a loopback if another loopback is already active, if a test code is being transmitted, or if a BERT is active. You cannot use the **SRL**, **SRP**, or **SRDP** commands in-band.

The figure below illustrates the Remote Maintenance menu. You use the commands listed in this menu to set and reset remote loopbacks. You must have super-user, configuration, or maintenance privileges.

remote loopback commands

```
                        REMOTE MAINTENANCE MENU

SRL             - Set Remote Line Loop Back
SRP             - Set Remote Payload Loop Back
SRDP<n>         - Set Remote Data Port Loop Back, n = 1
RST1            - Reset Remote Loop Back

SQC/S3C/S1C/S0C - Send Test Codes at NI: QRS, 3/24, 1 ,0
S5C<n>          - Send 511 Test Code in Data Port <n> Bit Stream
S2C<n>          - Send 2047 Test Code in Data Port <n> Bit Stream
RTC             - Reset Test Codes

BTQ/BT3/BT1/BT0 - Activate BERT using Test Codes: QRS, 3/24, 1 ,0
BT5<n>          - Activate BERT using 511 at Data Port n = 1
BT2<n>          - Activate BERT using 2047 at Data Port n = 1
```

SRL	Set a remote line loopback.
SRP	Set a remote payload loopback.
SRDP1	Set a remote data port loopback on data port 1.

To reset a remote loopback, enter **RST1**.

You may receive one or more of the following messages when setting or resetting remote loopbacks.

SENDING LOOP BACK SET CODE — The DataSMART is requesting a loopback.

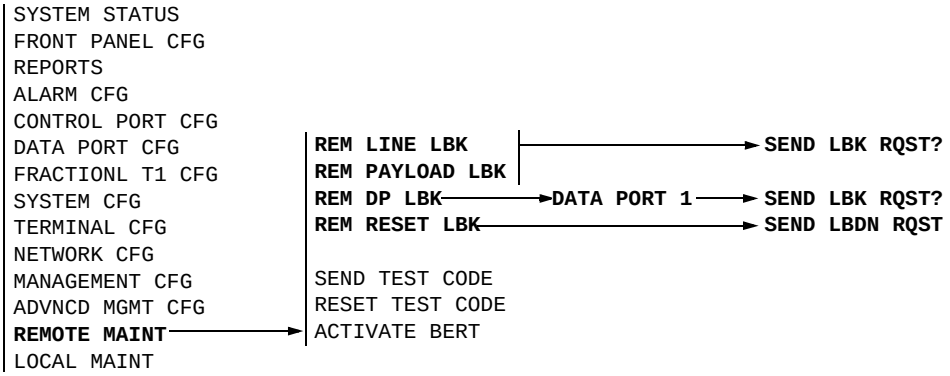
REMOTE LOOP BACK IS SET— The remote loopback is set.

UNABLE TO CONFIRM REMOTE LOOP BACK IS SET — The DataSMART tried to set the remote loopback but was unable to confirm that the loopback was set.

UNABLE TO SET REMOTE LOOP BACK — The DataSMART cannot set a loopback because a loopback is already set, a test code is being generated, or a BERT is active.

Using the front panel

To set remote loopbacks from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until REMOTE MAINT appears in the display.
3. Push Select. REM LINE LBK appears in the display.
4. Push Next or Previous until the desired loopback appears in the display.
5. Push Select. If you select the remote data port loopback, you must select the desired data port. Push Next or Previous until the desired data port appears in the display, then push Select.
6. A query asks if you really want to set the loopback. Push Select to set the loopback. LOOPBACK SET appears in the display.
7. If you want to reset a remote loopback (turn the loopback off), push Select when REM RESET LBK appears in the display. You will be asked to verify this selection. Push Select again.

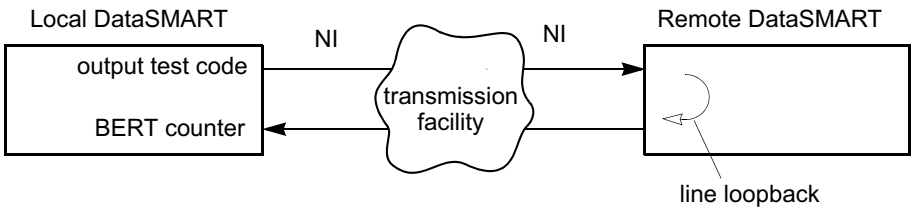
   When you send a request to set or reset a loopback, you will receive one of several responses:

SENDING RQST	The DataSMART is in the process of sending the request.
NO CONFIRMATION	The DataSMART sent the request, but was unable to confirm that the loopback was set or reset.
LPBK CONFIRMED	The DataSMART sent the request and the loopback was confirmed as set or reset.
UNABLE TO SEND	The DataSMART is unable to send the request because a loopback is already set, a test code is being sent, or a BERT is active.

Using test codes and BERTs

BERTs in a point-to-point application

When you set a remote loopback in a far-end device, you'll usually want to run a bit error rate test (BERT) on the looped signal. A BERT allows you to send a test code through a looped back line, then counts the errors returned in the signal. For example, the figure below illustrates how you might use a BERT in conjunction with a line loopback.



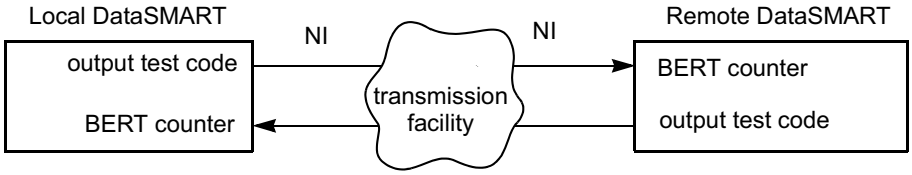
To use a BERT in conjunction with a remote loopback, do the following:

1. Set the remote loopback. You can set a remote line or payload loopback to test the full T1 signal, or you can set a data port loopback to test the channels assigned to a specific data port.
2. Send test codes through the loop.

   To test the full T1 signal, assign all of the network interface channels to the terminal interface or assign them all to the data port. Then send one of the following test codes: QRS, 3 in 24, all 1s, or all 0s.

   To test the channels assigned to the data port, send a 511 or 2047 code on the data port channels.
3. Activate the BERT and monitor the BERT error report.
4. Exit BERT.
5. Reset the test codes.
6. Reset the loopback.

You can also use BERT in a bidirectional, point-to-point test. In this application, you set each DataSMART in the point-to-point connection to output specific test code. Then you activate BERT on that test code in each device. This allows you to test the T1 signal between the network interfaces of the two devices.



How BERTs work

When a BERT is first activated, the DataSMART initializes all counters to zero. It starts monitoring the incoming network signal for the specified test pattern. (In the case of a data port loopback, the DataSMART looks for the specified test pattern only on the channels mapped to the specified data port.)

When the DataSMART recognizes the test pattern, it begins tracking time and errors. The time counter continues to count even during time of sync loss. The time and error counters continue to count until they reach their maximum limit as specified below; they do not roll over.

You can exit BERT by typing Ctrl-C.

```
RM> btq
^C to TERMINATE
SEARCHING FOR PATTERN
Pattern Detected
   TEST     BIT  ERRORED   BURSTY  SEV ERR  UNAVAIL   TOTAL BIT
SECONDS  ERRORS  SECONDS  SECONDS  SECONDS  SECONDS      ERRORS
-------  ------  -------  -------  -------  -------   ---------
      1       0        0        0        0        0           0
      2       0        0        0        0        0           0
      3       0        0        0        0        0           0
      4       0        0        0        0        0           0
      5       0        0        0        0        0           0
      6       0        0        0        0        0           0
      7       0        0        0        0        0           0
      8       1        1        0        0        0           1
      9       3        2        1        0        0           4
     10       5        3        2        0        0           9
     11       6        4        3        0        0          15
     12       5        5        4        0        0          20
     13       5        6        5        0        0          25
     14       5        7        6        0        0          30
     15       4        8        7        0        0          34
     16       0        8        7        0        0          34
     17       0        8        7        0        0          34
     18       0        8        7        0        0          34
     19       0        8        7        0        0          34
     20       0        8        7        0        0          34
```

Field	Description
TEST SECONDS	The number of seconds, up to 2^{32} maximum, that the DataSMART has been running the test after first detecting the test pattern.
BIT ERRORS	The number of bit errors, up to 65,535 maximum, that have occurred in the current second.
ERRORED SECONDS	The number of errored seconds, up to 65,535 maximum, that have occurred since the DataSMART first detected the test pattern.
BURSTY SECONDS	The number of bursty errored seconds, up to 65,535 maximum, that have occurred since the DataSMART first detected the test pattern.
SEV ERR SECONDS	The number of severely errored seconds, up to 65,535 maximum, that have occurred since the DataSMART first detected the test pattern.
UNAVAIL SECONDS	The number of unavailable seconds, up to 65,535 maximum, that have occurred since the DataSMART first detected the test pattern.

Field	Description
TOTAL BIT ERRORS	The running total of bit errors, up to 2^{32} maximum, that have occurred since the DataSMART first detected the test pattern.

Command-line access

You set and reset test codes and activate a BERT by using the commands listed in the Remote Maintenance menu. You must have super-user, configuration, or maintenance privileges to use these commands.

```
                        REMOTE MAINTENANCE MENU

SRL              - Set Remote Line Loop Back
SRP              - Set Remote Payload Loop Back
SRDP<n>          - Set Remote Data Port Loop Back, n = 1 .. 4
RST1             - Reset Remote Loop Back

SQC/S3C/S1C/S0C - Send Test Codes at NI: QRS, 3/24, 1 ,0
S5C<n>           - Send 511 Test Code in Data Port <n> Bit Stream
S2C<n>           - Send 2047 Test Code in Data Port <n> Bit Stream
RTC              - Reset Test Codes

BTQ/BT3/BT1/BT0 - Activate BERT using Test Codes: QRS, 3/24, 1 ,0
BT5<n>           - Activate BERT using 511 at Data Port n = 1 .. 4
BT2<n>           - Activate BERT using 2047 at Data Port n = 1 .. 4
```

test code commands

BERT commands

Each test code is sent out framed. To set and reset test codes:

SQC	Send framed QRS code out the network interface.
S3C	Send framed 3-in-24 code out the network interface.
S1C	Send all 1s out the network interface. This may be required by the carrier.
S0C	Send all 0s out the network interface.
S2C1	Send 2047 code in the channels assigned to data port 1.
S5C1	Send 511 code in the channels assigned to data port 1.
RTC	Reset the test code generation.

To activate a BERT on the test codes:

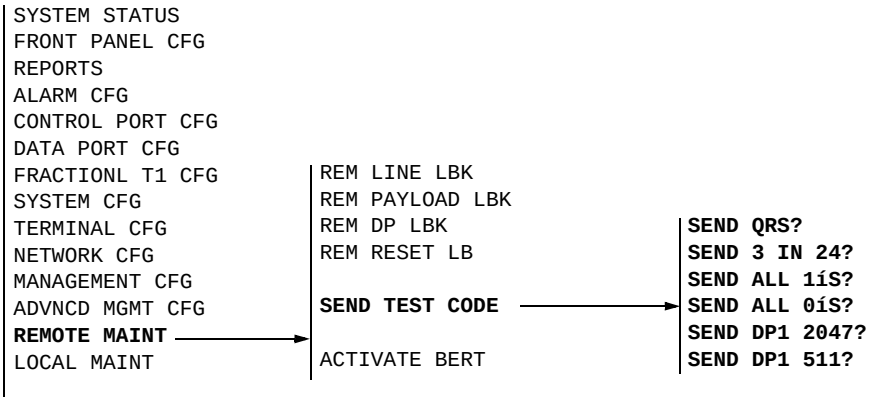
BTQ	Activate a BERT on QRS test code.
BT3	Activate a BERT on 3-in-24 test code.
BT1	Activate a BERT on all 1s test code.
BT0	Activate a BERT on all 0s test code.
BT51	Activate a BERT on 511 test code in channels assigned to data port 1.
BT21	Activate a BERT on 2047 test code in channels assigned to data port 1.

To de-activate or exit a BERT, enter Ctrl-C.

When you first activate a BERT, you will receive the message SEARCHING FOR PATTERN. When the DataSMART recognizes the test pattern, the BERT report will appear on the display.

Front-panel access

To set and reset test codes from the front panel, use these steps.



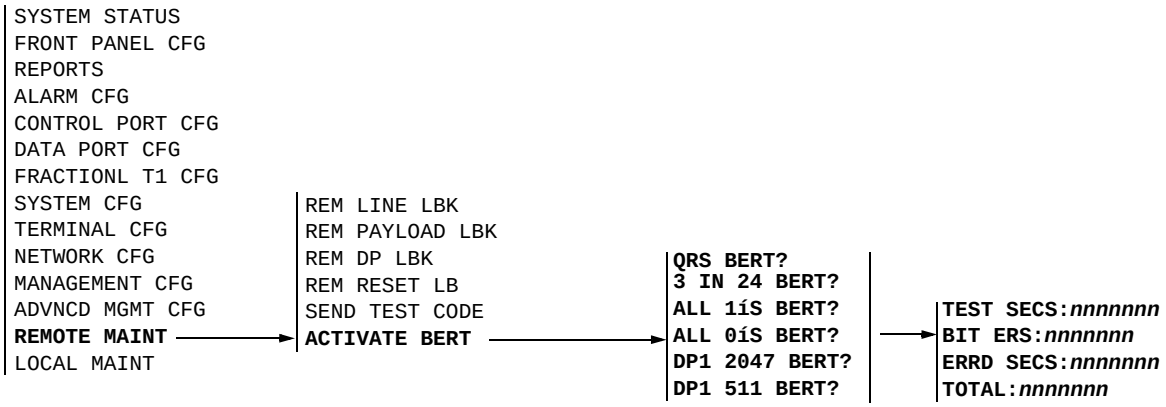
1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until REMOTE MAINT appears in the display.
3. Push Select. REM LINE LBK appears in the display.
4. Push Next or Previous until SEND TEST CODE appears in the display.
5. Push Select. SEND QRS? appears in the display.
6. Push Next or Previous until the desired test code appears in the display.
7. Push Select to send the test code. You may receive one of the following responses:

UNABLE TO SET	This means DataSMART is not able send the test code to the far-end device because another test condition exists.
NO CHAN ASSIGNED	This means DataSMART is not able to send 2047 or 511 test code because the data port has no assigned channels.

8. After a few seconds, the message RESET TEST CODE appears. Push Select when you want to stop sending test code. You are asked to confirm the selection. You may receive the following response:

UNABLE TO CLEAR	The DataSMART is not able to reset the test code.

To activate a BERT, use the following steps. To deactivate a BERT, push Escape.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until REMOTE MAINT appears in the display.
3. Push Select. REM LINE LBK appears in the display.
4. Push Next or Previous until ACTIVATE BERT appears in the display.
5. Push Select. QRS BERT? appears in the display.
6. Push Next or Previous until the desired BERT appears in the display.
7. Push Select to activate the BERT. The display will show SEARCHING, indicating that the DataSMART is searching for the specified test code in the incoming signal. When it finds it, the first readout in the list below appears. Push Next or Previous to see the other readouts. The readouts are updated dynamically as long as the BERT is active.

TEST SECS: *nnnnnnn*	The number of seconds, up to 65,535 maximum, since the test pattern was first detected.
BIT ERS: *nnnnnnn*	The number of bit errors, up to 65,535 maximum, that have occurred in the current second.
ERRD SECS: *nnnnnnn*	The number of errored seconds, up to 65,535 maximum, that have occurred since the DataSMART first detected the test pattern.
TOTAL: *nnnnnnn*	The total number of bit errors since the test code was first detected.

C H A P T E R

8 Using network management

The DataSMART DSUs support network management via Telnet and the Simple Network Management Protocol (SNMP).

This chapter tells you how to:

- Configure for Telnet
- Configure for SNMP

About obtaining IP addresses

The procedures in this chapter require a valid IP address. If there is a network administrator or system administrator at your company, he or she is responsible for obtaining valid IP addresses and issuing them to you. All IP-based networks require IP addresses to be unique. Because of this requirement, **you must obtain a valid IP address for your unit to function; your unit's default IP addresses will not work.**

If there is no one at your company who is responsible for obtaining valid IP addresses, contact your Internet service provider. **Kentrox cannot issue IP addresses for you.**

Basic network management (Telnet)

To manage DataSMART with SNMP or Telnet, you must configure the unit to operate with TCP/IP networks. Configuring the unit for management via Telnet is the first step in configuring for SNMP.

The DataSMART must be configured to operate in a TCP/IP network to use the base level of network management.

To manage a DataSMART with SNMP or Telnet, it must be configured to operate with TCP/IP networks. The minimal IP network configuration for each unit (enough to enable Telnet and the ping response) consists of:

- Setting the IP interface protocol
- Setting the IP address, netmask, and default router address for each IP interface the unit will use
- Configuring the IP network interface used for managing the unit
- Setting the Telnet password

If you want to use SNMP to manage your DataSMART unit, these steps are also required:

- Enabling the SNMP agent
- Setting the SNMP read, write, and trap community strings
- Setting up IP address screening, if extra IP network security is desired

Command-line access

The DataSMART has two IP management configuration menus:

- The Management Configuration menu contains the commands needed to set up a basic IP network interface and communicate with the unit via Telnet.
- The Advanced Management Configuration menu contains the commands needed to set up SNMP communications with a DataSMART unit.

Super-user or configuration access is required to use either menu.

Enter **MC** to display the Management Configuration menu.

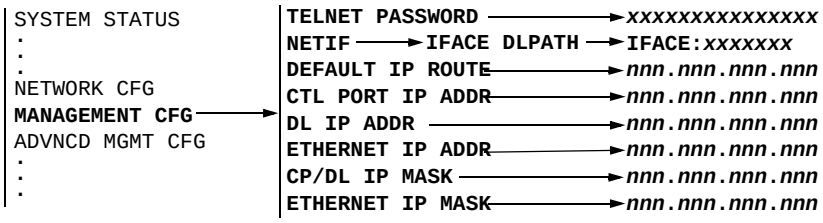
```
                MANAGEMENT CONFIGURATION MENU

TPW:<str>           - Set Telnet Password, str=0 to 15 characters
                      0 characters disables Telnet
NETIF:<p>[,<dl>[,<spd>]]
                    - Set IP Network Interface Paths
                      <p> = N, E, PS, S, D, ES, ED, ESD, PSD, or SD
                      N = None, E = Ethernet, P = PPP, S = SLIP,
                      D = Datalink  -  if Datalink, use dl and spd
                      <dl> = F (FDL), 1-24 (DS0 Tslot) - if DS0, use spd
                      <spd> = 56 (56k of DS0 Tslot), 64 (All of Tslot)

IPR:<ipa>           - Set Default Route IP Address
IPA:<p>,<ipa>       - Set IP Addresses
IPM:<p>,<mask>      - Set IP Masks
                      p = E (Ether), C (PPP/SLIP), D (Datalink)
                      <ipa> and <mask> = n.n.n.n, n = 0 .. 255 (dec)
                      <ipa> for Datalink is IP Address of remote unit
                      <mask> is the same for Ctl Port and Datalink

AMC                 - Advanced Management Configuration Menu
MCV                 - View Management Configuration
```

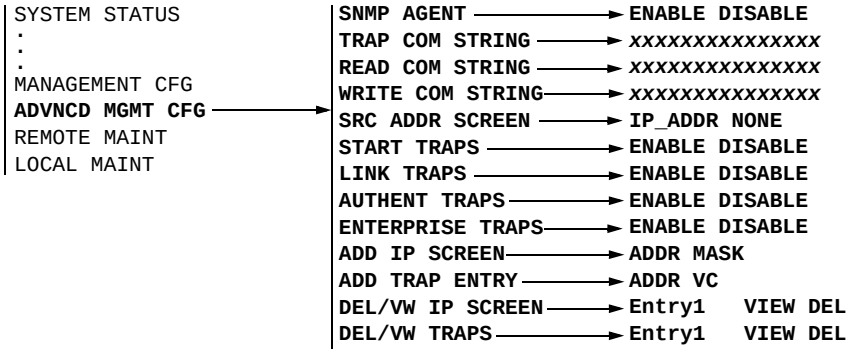
Enter **AMC** to display the Advanced Management Configuration menu.

```
           ADVANCED MANAGEMENT CONFIGURATION MENU

ESNMP/DSNMP         - Enable/Disable SNMP Agent

TCS:<str>           - Set SNMP Trap Comm String, str=1 to 15 chars
RCS:<str>           - Set SNMP Read Comm String, str=1 to 15 chars
WCS:<str>           - Set SNMP Write Comm String, str=1 to 15 chars

SSA:<p>             - Set Packet Screening via Source Address
                      p = I (IP Addr), N (None)
TRAP:<c>,<t>        - SNMP Trap Generation c = E (Enable), D (Disable)
                      t = S (Start), L (Link), A (Auth), E (Enterprise)
ADD:T,<ip>[,dlci]   - Add IP Address to Trap Dest List
                      <dlci> = optional identifier for Data Link Traps
ADD:I,<ip>[,mask]   - Add IP Address to Screening List
DEL:<l>,<ip>        - Delete Address from Screening or Trap Dest Lists
                      <l> = I (IP Screen List), T (Trap Dest List)
                      <ip> and [mask] = n.n.n.n, n = 0.. 255 (dec)
                      [mask] used only for IP Screen List (Optional)

AMCV                - View Advanced Management Configuration
```

Front-panel access

Front-panel access is provided through the MANAGEMENT CFG and ADVNCD MGMT CFG menus.





View the current settings

Before changing any management parameters, you may want to look at the current settings. You do this by executing the **MCV** command. This command displays the View Management Configuration screen. To see the Telnet password, you must have super-user privileges. To see advanced management parameters, enter the **AMCV** command.

```
          VIEW MANAGEMENT CONFIGURATION

Telnet Password  IP Interface Paths       DL Path
---------------  -----------------------  ------------
                 NONE                     NONE

CP IP Addr        DL IP Addr        CP & DL IP Mask   IP Default Router
----------------  ----------------  ----------------  --------------
192.0.2.1         192.0.2.1         255.255.255.0     192.0.2.2

Ethernet IP Addr  Ethernet IP Mask
----------------  ----------------
192.0.2.1         255.255.255.0
```

```
       VIEW ADVANCED MANAGEMENT CONFIGURATION

SNMP Agent  Trap Comm String   Read Comm String   Write Comm String
----------  -----------------  -----------------  -----------------
DISABLED    snmptrap           public             private

Addr Screening  Traps Enabled
--------------  -----------------------------------
NONE            Start Link Authentication Enterprise

IP Source Address Screening        Trap Destination
---------------------------------  ------------------------
IP Addr           IP Mask          IP Addr           VC
---------------   ---------------  ----------------  ------
                                   192.0.2.2              0
```

Field	Description
Telnet Password	This field tells you the current Telnet password. If there is no Telnet password, the Telnet Server will not be active and you will not be able to Telnet to the unit.
IP Interface Paths	This field tells you the currently selected IP interfaces. Possible values you may see in this field are ETHER, PPP, SLIP, DATALINK, or NONE.
DL Path	This field tells you which IP management data link is selected. Possible values are DS0 MODE, FDL MODE, or NONE.
CP IP Addr	This field tells you the control port IP address the unit is currently using for SLIP and PPP.
DL IP Addr	This field tells you the data link IP address the unit is currently using.
CP & DL IP Mask	This field tells you the control port and data link IP netmask the unit is currently using for SLIP, PPP, and the data link.
IP Default Router	This field tells you the address of the IP default router, which the unit must send packets to in order to get them into the IP network.
Ethernet IP Address	This field shows the Ethernet IP address the unit is currently using.
Ethernet IP Mask	This field shows the Ethernet IP netmask the unit is currently using.
SNMP Agent	This field tells you if the SNMP Agent is enabled or disabled.
Trap Comm String	This field tells you the current value of the SNMP Trap Community String. The default value is “snmptrap”.
Read Comm String	This field tells you the current value of the SNMP Read Community String. The default value is “public”.
Write Comm String	This field tells you the current value of the SNMP Write Community String. The default value is “private”.
Addr Screening	This field tells you if IP addresses are currently being screened by the unit.
Traps Enabled	This field tells you which SNMP trap types will be sent if the SNMP Agent is enabled. The trap types are Start, Link, Authentication, Enterprise, or any combination of the preceding.
IP Source Addr Screening: IP Addr	This field shows which IP addresses are allowed to communicate with the unit. This field can have up to ten entries. Duplicate entries are not valid.
IP Source Addr Screening: IP Mask	This field contains the IP mask that determines which IP subnet the unit belongs to. If a mask is present, any other IP host in the subnet is allowed to communicate with the unit. This field can have up to ten entries. Duplicate entries are not valid.
Trap Destination: IP Addr	This field tells you which IP addresses the unit sends traps to. This field can have up to ten entries. Duplicate entries are valid.
Trap Destination: VC	This field tells you which virtual circuit (VC) the unit uses to send out traps. It is valid only for the data link IP interface.

About IP addressing

To send and receive data across the IP network, every device (or *host*, in IP terminology) on the network requires a unique IP address. An IP address consists of four decimal numbers between 0 and 255, separated by periods. This convention is called *dotted decimal notation*. Each address is composed of two parts: a network part, which identifies the subnet containing the host; and a host part, which identifies the actual host device.

An IP address mask, also called a *netmask,* is used in conjunction with the IP address to determine which part of the address is the network part and which is the host part. In the examples in this guide, the netmask is 255.255.255.0, which sets the first three numbers of the IP address as the network part and the last number as the host part.

Typically, you get IP addresses from your network or system administrator or Internet Service Provider (ISP). If you are the network or system administrator, get a network address from the InterNIC. **Kentrox cannot provide you with IP addresses.** Assign an IP address to each host in the IP network.

Sample configurations with IP addresses

The following examples illustrate different ways of configuring DataSMART units for IP management.

Sample applications

The four examples in this section are:

- Dedicated T1 line or Frame Relay access, remote site managed in-band via Ethernet connection to router: see page 169.
- Dedicated T1 line, central site managed via Ethernet, remote unit managed in-band via 8-Kbps DS0 data link: see page 170.
- Dedicated T1 (ESF) line, central site managed via serial port using PPP, remote unit managed in-band via 4-Kbps FDL data link: see page 171.
- Dedicated Fractional T1 line, CSU at central site managed via Ethernet, remote unit managed via 56-Kbps DS0 data link: see page 172.

Each example explains how to:

- Assign network interface channels on the DataSMART DSU
- Configure the DataSMART network interface
- Assign IP addresses and IP netmasks
- Set up a Telnet password

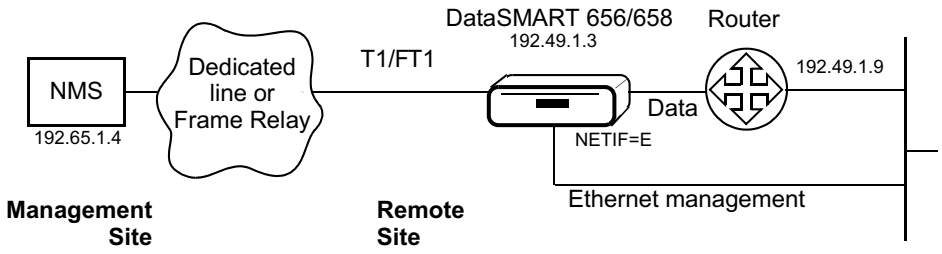
Example 1—Remote site DSU managed via Ethernet, SNMP traps enabled

Example 1 illustrates how to set up an Ethernet-managed DataSMART unit at a remote site. The IP management path passes through the DataSMART unit, through the router, and onto the LAN where the DataSMART unit picks up packets addressed to it. See Figure 14.

The DataSMART unit can be a DataSMART 656 or a DataSMART 658. The configuration steps are the same for both units.

Source address screening setup (steps 8 and 9) and SNMP trap setup (steps 10-12) are optional.

Figure 14—DSU application centrally managed via Ethernet



Configuration Commands - Remote Site Use these commands to set up NI channel assignments and IP network management for the DataSMART unit at the remote site (right side of Figure 14):

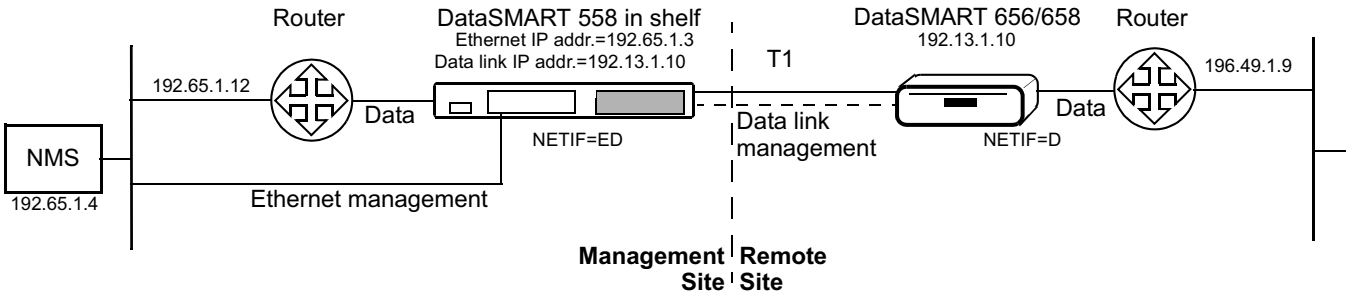
1. Type **ADP1:64,1-24** to assign all 24 NI channels to the data port at 64 Kbps.
2. Type **LXA** to load network interface configuration Table A into the unit.
3. Type **NETIF:E** to set up the Ethernet IP management interfaces.
4. Type **IPA:E, 192.49.1.3** to set the DataSMART's Ethernet IP address.
5. Type **IPM:E, 255.255.255.0** to set the Ethernet IP netmask (to the default).
6. Type **IPR: 192.49.1.9** to identify the DataSMART's default router.
7. Type **TPW: KENTROX** to set the Telnet password to KENTROX (all caps).
8. (Source address screening setup—optional)
   Type **ADD:I, 192.65.1.4** to add the NMS IP address to the source address screening list, ensuring that the NMS can manage the DataSMART.
9. Type **SSA:I** to enable source address screening, ensuring that only the hosts in the source address screening list (i.e., the NMS) can manage the DataSMART.
10. (SNMP trap setup—optional)
    Type **ADD:T, 192.65.1.4** to send traps to the NMS.
11. Type **ESNMP** to enable the SNMP agent on the DataSMART (enabled by default).
12. Type **TRAP:E,S, TRAP:E,L, TRAP:E,A,** and **TRAP:E,E** to enable start, link, authentication, and enterprise traps. (All are enabled by default.)

Example 2—DSU centrally managed via Ethernet and DS0 data link

In Example 2, both DataSMART units are set up as full-rate DSUs. The network management system (NMS) manages the near-end DataSMART unit via Ethernet. Manage the far-end unit in-band via the data link, which "borrows" 8 Kbps from time slot 24, leaving 1528 Kbps bandwidth available for data on the T1 line. See Figure 15.

The DataSMART unit at either end can be a DataSMART 558 in a shelf, a DataSMART 656, or a DataSMART 658. The configuration steps are the same for all these units.

Figure 15—DSU application centrally managed via Ethernet and DS0 data link



Configuration Commands - Management Site Use these commands to set up NI channel assignments and IP network management for the DataSMART unit at the management site (left side of Figure 15):

1. Type **ADP1:64,1-24** to assign all 24 NI channels to the data port at 64 Kbps.
2. Type **LXA** to load network interface configuration Table A into the unit.
3. Type **NETIF:ED,24** to set up two IP management interfaces: Ethernet and a data link IP interface borrowing 8 Kbps from time slot 24.
4. Type **IPA:D, 192.13.1.10** to tell the DataSMART to send IP traffic addressed to 192.13.1.10 (the remote DataSMART's data link IP address) via the IP data link.
5. Type **IPM:C, 255.255.255.0** to set the data link IP netmask (to the default).
6. Type **IPA:E, 192.65.1.3** to set the DataSMART's Ethernet IP address.
7. Type **IPM:E, 255.255.255.0** to set the Ethernet IP netmask (to the default).
8. Type **IPR: 192.65.1.12** to identify the DataSMART's default router.
9. Type **TPW: KENTROX** to set the Telnet password to KENTROX (all caps).

Configuration Commands - Remote Site Use these commands to set up the remote site's DataSMART unit (right side of Figure 15):

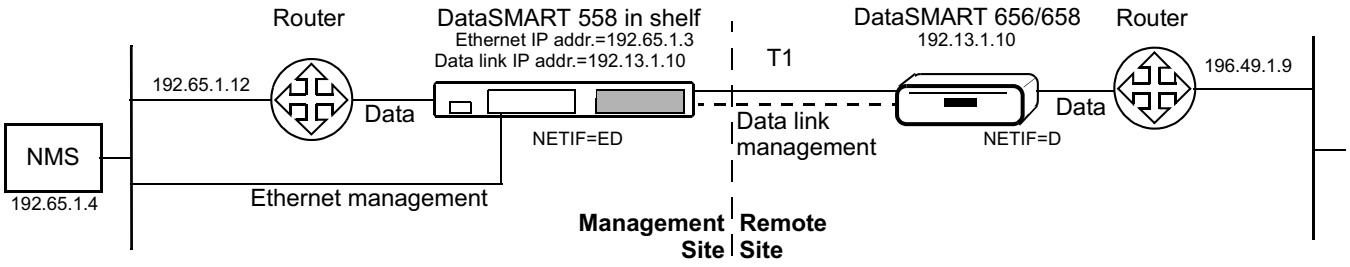
1. Type **ADP1:64,1-24** to assign all 24 NI channels to the data port at 64 Kbps.
2. Type **LXA** to load network interface configuration Table A into the unit.
3. Type **NETIF:D,24** to set up a data link borrowing 8 Kbps from time slot 24.
4. Type **IPA:D, 192.13.1.10** to set the DataSMART's data link IP address.
5. Type **IPM:C, 255.255.255.0** to set the data link IP netmask (to the default).
6. Type **TPW: KENTROX** to set the Telnet password to KENTROX (all caps).

Example 3—Fractional T1 DSU managed via Ethernet and DS0 data link

In Example 3, both DataSMART units are set up as 672-Kbps fractional T1 DSUs. The NMS manages the near-end DataSMART unit via Ethernet. Manage the far-end unit in-band via the data link, which runs on idle channel 24 at 56 Kbps. See Figure 16.

The DataSMART unit at either end can be a DataSMART 558 in a shelf, a DataSMART 656, or a DataSMART 658. The configuration steps are the same for all these units.

Figure 16—Fractional T1 DSU application managed via Ethernet and DS0 data link



Configuration Commands - Management Site Use these commands to set up NI channel assignments and IP network management for the DataSMART unit at the management site (left side of Figure 16):

1. Type **ADP1:56,1-12** to assign NI channels 1-12 to the data port at 56 Kbps.
1. Type **ANI 13-24:I** to assign NI channels 13-24 to idle.
2. Type **LXA** to load network interface configuration Table A into the unit.
3. Type **NETIF:ED,24,56** to set up two IP management interfaces: Ethernet and a data link IP interface using time slot 24 at 56 Kbps.
4. Type **IPA:D, 192.13.1.10** to tell the DataSMART to send IP traffic addressed to 192.13.1.10 (the remote DataSMART's data link IP address) via the IP data link.
5. Type **IPM:C, 255.255.255.0** to set the data link IP netmask (to the default).
6. Type **IPA:E, 192.65.1.3** to set the DataSMART's Ethernet IP address.
7. Type **IPM:E, 255.255.255.0** to set the Ethernet IP netmask (to the default).
8. Type **IPR: 192.65.1.12** to identify the DataSMART's default router.
9. Type **TPW: KENTROX** to set the Telnet password to KENTROX (all caps).

Configuration Commands - Remote Site Use these commands to set up the remote site's DataSMART unit (right side of Figure 16):

1. Type **ADP1:56,1-12** to assign NI channels 1-12 to the data port at 56 Kbps.
2. Type **LXA** to load network interface configuration Table A into the unit.
3. Type **NETIF:D,24,56** to set up a data link IP interface using time slot 24 at 56 Kbps.
4. Type **IPA:D, 192.13.1.10** to set the DataSMART's data link IP address.
5. Type **IPM:C, 255.255.255.0** to set the data link IP netmask (to the default).
6. Type **TPW: KENTROX** to set the Telnet password to KENTROX (all caps).

Example 4—Dedicated line CSU centrally managed via control port and FDL

In Example 4, the T1 service must have ESF line coding, and the Facility Data Link (FDL) must be available end-to-end. All channels on both DataSMART units are set to data-type channels on the terminal interface. The applications at either end can be ISDN PRI, Common Channel Signaling (CCS), or other applications that require a clear channel. Manage the near-end unit using PPP on the asynchronous control port. Manage the far-end unit in-band in the Facility Data Link at 4 Kbps. See Figure 17.

The units in this example can be DataSMART 558 or 658 or M-PATH 537 or 538 units.

The headquarters site has two DataSMART units, each connected via T1 and a data link to its own remote site. The units can be installed in the same shelf or can be daisy-chained 658s. The network port host at the headquarters site can be a terminal server, a host with PPP communications software, a router, or a modem. It communicates directly with unit HQ 1 in Slot 1, and over the shelf's backplane to the unit HQ 2 in Slot 2.

The branch sites are identical, except for the IP addresses.

All units must have ESF framing and B8ZS line coding on the NI and TI (see Chapter 5).

Figure 17—Dedicated line CSU centrally managed via control port and FDL

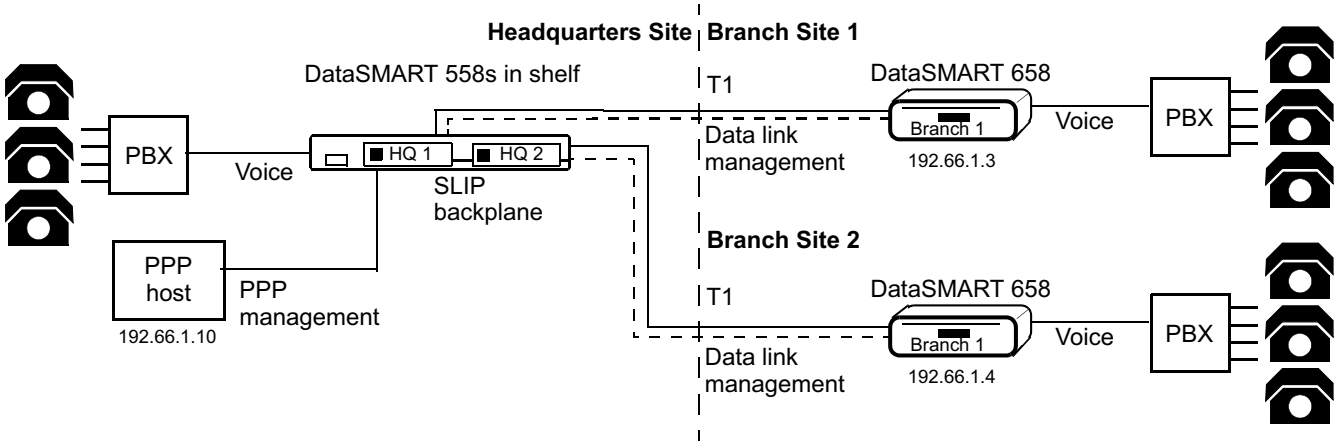


Table 8—Parameters and addresses for a multi-site example

Unit name	Use NETIF parameters	Linked to unit(s)...	Data link IP address	Control port IP address
HQ 1	PSD,F	Network Port via PPP; HQ 2 via SLIP backplane; Branch 1 via data link	192.66.1.3	192.66.1.11
HQ 2	SD,F	HQ 1 via SLIP backplane; Branch 2 via data link	192.66.1.4	192.66.1.12
Branch 1	D,F	HQ 1 via data link	192.66.1.3	—
Branch 2	D,F	HQ 2 via data link	192.66.1.4	—

Configuration Commands - Headquarters Site Log into the unit farthest away from the controller (or farthest away from the head of the daisy-chain) and follow all the steps that apply to that unit. Then log out and log into the next unit in line, and so on. The controller should be the last unit configured.

Use the following commands to set up NI channel assignments and IP network management for DataSMART units HQ 1 and HQ 2 (left side of Figure 17):

1. On both units, type **ANI1-24:D** to assign all 24 NI channels to the terminal interface, data-type channels.
2. On both units, type **LXA** to load network interface configuration Table A.
3. On unit HQ 2, type **NETIF:SD,F** to set up a control port IP management interface for the SLIP backplane and a data link IP interface using the FDL.
4. On unit HQ 2, type **IPA:C, 192.66.1.12** to set unit HQ 2's control port IP address for the SLIP backplane.
5. On unit HQ 2, type **IPA:D, 192.66.1.4** to tell unit HQ 2 to send all IP traffic addressed to 192.66.1.4 (unit Branch 2's data link IP address) via the IP data link.
6. On unit HQ 1, type **NETIF:PSD,F** to set up IP management interfaces for the control port using PPP; the SLIP backplane; and a data link using the FDL.
7. On unit HQ 1, type **IPA:C, 192.66.1.11** to set unit HQ 1's control port IP address for both PPP and the SLIP backplane.
8. On unit HQ 1, type **IPA:D, 192.66.1.3** to tell unit HQ 1 to send all IP traffic addressed to 192.66.1.3 (unit Branch 1's data link IP address) via the IP data link.
9. On both units, type **IPR: 192.66.1.10** to identify the DataSMART's default route, via the network port host.
10. On both units, type **IPM:C, 255.255.255.0** to set the control port/data link IP netmask (to the default).
11. On both units, type **TPW: KENTROX** to set the Telnet password to KENTROX (all caps).

TIP
When manually configuring more than one DataSMART 500 unit in the same shelf, set the IP network interface for the last unit (farthest away from the controller) first, and then set up the IP network interfaces in reverse order, configuring the controller last. You may not be able to access a shelf unit set to NETIF:N through a controller that is using SLIP.

Configuration Commands - Branch Sites Use these commands to set up the branch site DataSMART units (right side of Figure 17):

1. On both units, type **ANI1-24:D** and **LXA** to set up and load the NI configuration.
2. On both units, type **NETIF:D,F** to set up a data link IP interface using the FDL.
3. On unit Branch 1, type **IPA:D, 192.66.1.3** to set the data link IP address.
4. On unit Branch 2, type **IPA:D, 192.66.1.4** to set the data link IP address.
5. On both units, type **IPM:C, 255.255.255.0** to set the control port/data link IP netmask (to the default).
6. On both units, type **TPW: KENTROX** to set the Telnet password to KENTROX (all caps).

Choosing an IP network interface protocol

DataSMART 656 and 658 DSUs allow you to choose one or more of the following IP network interface protocols:

- Ethernet
- PPP or SLIP over the unit's DCE or DTE control port
- Data link over the T1 connection

Each network interface requires you to enter a separate IP address for each unit and an IP netmask. The Control Port/Data Link (CP/DL) netmask is used for both the control port (PPP/SLIP) and the data link.

Table 9—IP network interface options

Option	Command Line	Front Panel	IP Addresses	IP Netmasks	Use this option when...
Ethernet	**E**	ETHERNET	Ethernet	Ethernet	A single DataSMART unit connects to the NMS or router via Ethernet
Ethernet-Data Link	**ED**	ETH-DL	Ethernet, Data Link	Ethernet, CP/DL	Same as above, also managing a remote DataSMART unit in-band via data link
PPP-SLIP	**PS**	PPP-SLIP	Control Port	CP/DL	The DataSMART unit connects to the router or network port host via PPP and is not in the middle or end of a daisy chain.
PPP-SLIP-Data Link	**PSD**	P-SLIP-DL	Control Port, Data Link	CP/DL	Same as above, also managing a remote DataSMART unit in-band via data link
SLIP	**S**	SLIP	Control Port	CP/DL	The DataSMART unit is in the middle or end of a daisy chain or it connects to the network host directly using SLIP
SLIP-Data Link	**SD**	SLIP-DL	Control Port, Data Link	CP/DL	Same as above, also managing a remote DataSMART unit in-band via data link
Ethernet-SLIP	**ES**	ETH-SLIP	Ethernet, Control Port	Ethernet, CP/DL	The DataSMART is at the head of a daisy-chain and connects to the NMS or router via Ethernet
Ethernet-SLIP-Data Link	**ESD**	E-SLIP-DL	Ethernet, Control Port, Data Link	Ethernet, CP/DL	Same as above, also managing a remote DataSMART unit in-band via data link
Data Link	**D**	DL	Data Link	CP/DL	The DataSMART is remotely managed in-band via data link
No IP (ASCII mode)	**N**	NONE	N/A	N/A	You are not using SNMP management

Daisy-chaining units

You can manage multiple DataSMART units at the same site from a single terminal or Ethernet port by interconnecting them via their DCE and DTE control ports. You connect the DTE port of one unit to the DCE port of the next unit, and so on.

IP network interfaces that include a data link

The data link uses part of the T1 data stream to connect units at either end of a data-linked pair. The near-end unit can be connected directly to a router, terminal or network management system via PPP, SLIP, or Ethernet, or can be daisy-chained to other near-end units. (Daisy-chained units communicate with each other using SLIP.) The near-end unit is configured as **SD**, **ED**, **ESD**, or **PSD**. The far-end unit is always configured as **D**. This prevents DataSMART units from trying to manage each other, or two different control devices trying to manage the same DataSMART unit.

If the IP network interface includes a data link, you must enter an IP address and IP netmask for the data link (see "Setting the IP address" on page 179 and "Setting the IP netmask" on page 180).

The data link can be assigned to:

- The Facility Data Link (FDL) which runs at 4 Kbps and is available only if both the near-end and far-end DataSMART units are using Extended Super Frame (ESF) NI framing (see "Specifying NI framing format" on page 72).

- One of the T1 channels (time slots) that is idle or assigned to a data port. You can set a channel to 56 Kbps or 64 Kbps; if the channel has been assigned to a data port, use the same data speed setting you used when setting up the NI channel (see "Planning the channel assignment" on page 96).

  If the channel is idle, the data link runs at 56 Kbps or 64 Kbps, as you set it with the **NETIF** command or the front panel.

  If the channel is assigned to a data port and is set to 56 Kbps, the data link uses the "spare" 8 Kbps on that channel. Data port timing (see page 44) is not available if the data link is assigned to a data port.

  If the channel is assigned to a data port and is set to 64 Kbps, the data link takes 8 Kbps and the actual data link transfer rate is automatically reduced to 56 Kbps. You do not have to reconfigure either unit, and you can still get 64 Kbps on all the other data port channels. Data port timing (see page 44) is not available if the data link is assigned to a data port.

IP network interfaces that include Ethernet

The **E** (Ethernet), **ES** (Ethernet and SLIP), **ED** (Ethernet and Data Link), and **ESD** (Ethernet, SLIP and Data Link) protocols all require an Ethernet IP address and Ethernet IP netmask. See "Setting the IP address" on page 179 and "Setting the IP netmask" on page 180.

If you are connecting DataSMART 600 units in a daisy chain, the **ES** and **ESD** protocols let you use Ethernet to communicate to the unit at the head of the chain. All units in the chain communicate with each other via SLIP. Non-daisy-chained units should use the **E** and **ED** protocols instead.

IP network interfaces that use the control port

The following protocols let you control the DataSMART using IP over the control port:

- The **PS** (PPP and SLIP) and **PSD** (PPP, SLIP and Data Link) protocols use PPP to manage the near-end unit and Data Link protocol (if **PSD** is selected) to manage the far-end unit. If you are connecting DataSMART 600 units in a daisy chain, these

protocols let you use PPP to communicate to the unit at the head of the chain. All units in the chain communicate with each other via SLIP.

- The **S** (SLIP) and **SD** (SLIP and Data Link) protocols use SLIP to manage the near-end unit and Data Link protocol (if **SD** is selected) to manage the far-end unit. If you are setting up a daisy chain, all units in the chain communicate with each other via SLIP.

These four protocols, plus the **ES** (Ethernet and SLIP) and **ESD** (Ethernet, SLIP and Data Link) protocols, require an IP address and IP netmask for the control port (see "Setting the IP address" on page 179 and "Setting the IP netmask" on page 180).

Managing DataSMART units with ASCII mode

If you prefer to use ASCII mode instead of IP to manage DataSMART units, select **N** (None) for all daisy-chained units.

Selecting an IP network interface from the command line

IP network interfaces that include a data link

You select the IP network interface by using the **NETIF** command. There are two forms of the command, depending on whether you want an IP network interface that includes the IP management data link. You must have super-user or configuration privileges to use either form.

The command syntax is:

NETIF:*p*,*dl* [,*spd*]

p	Specify the protocol: **D** (Data Link) **SD** (SLIP and Data Link) **ED** (Ethernet and Data Link) **ESD** (Ethernet, SLIP and Data Link) **PSD** (PPP, SLIP and Data Link)
dl	Enter **F** to use the Facility Data Link (FDL) or a number from **1** to **24** to select a time slot for the data link.
spd	Enter **56** to set the data link data rate to 56 Kbps, or **64** to select 64 Kbps. If you specified F, this value is ignored.

IP network interfaces that do not include a data link

The command syntax is:

NETIF:*p*

p	Specify the protocol: **S** (SLIP) **E** (Ethernet) **PS** (PPP and SLIP) **ES** (Ethernet and SLIP) **N** (none)

Selecting the IP network interface from the front panel

The method for selecting the IP network interface is different for interfaces that include a data link and those that do not.

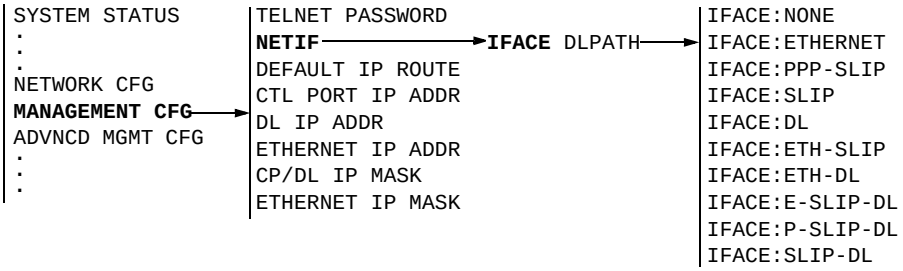
If you want to select NONE, ETHERNET, PPP-SLIP, SLIP, or ETH-SLIP, follow the steps in "Using the front panel to select the IP network interface" on page 177.

If you want to select DL, ETH-DL, E-SLIP-DL, P-SLIP-DL, or SLIP-DL, follow the steps in "Using the front panel to select the IP network interface" on page 177 and then follow the steps in "Using the front panel to specify the IP data link path" on page 178.

For more information about the available IP network interfaces, see Table 9 on page 174.

Using the front panel to select the IP network interface

To set the IP network interface from the front panel, use these steps.

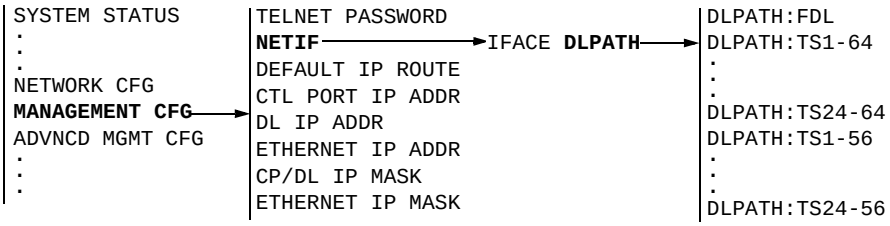


1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until MANAGEMENT CFG appears in the display.
3. Push Select. TELNET PASSWORD appears in the display.
4. Push Next or Previous until NETIF appears in the display.
5. Push Select. IFACE DLPATH appears in the display.
6. Push Next or Previous until IFACE is highlighted.
7. Push Select. The currently selected IP network interface appears in the display.
8. Push Next or Previous until the network interface you want is displayed, blinking with a question mark. Then push Select. The question mark disappears.
9. Push Escape. IFACE DLPATH appears in the display.
10. If you selected NONE, ETHERNET, PPP-SLIP, SLIP, or ETH-SLIP, go to step 11. Otherwise, go to the next procedure and specify the data link.
11. Push Escape. SET NETIF? appears in the display.
12. Push Select. NETIF SET appears in the display.

Using the front panel to specify the IP data link path

If your unit's IP network interface is DL, ETH-DL, E-SLIP-DL, P-SLIP-DL, or SLIP-DL, you need to select an IP data link and data rate. DataSMART units on both ends of the IP data link should use the same data link path specifications.

To specify the IP data link path from the front panel, use these steps.



1 Follow the procedure in"Using the front panel to select the IP network interface" on page 177.

2 Push Escape until IFACE DLPATH appears in the display.

3 Push Next or Previous until DLPATH is highlighted.

4 Push Select. The currently selected IP data link path appears in the display.

5 Push Next or Previous until the IP data link path you want is displayed, blinking with a question mark. Then push Select. The question mark disappears.

6 Push Escape. IFACE DLPATH appears in the display.

7 Push Escape. SET NETIF? appears in the display.

8 Push Select. NETIF SET appears in the display.

Setting the IP address

TIP
If you do not know what your IP address and IP netmask should be, ask your network administrator or system administrator. If you do not have a network or system administrator, obtain a set of valid IP addresses from your Internet service provider. ***Kentrox cannot issue IP addresses.***

The IP address is the unique address for a device in the IP network. The default IP address is 192.0.2.1. **You must change this IP address before adding the unit to an IP network.**

All units in a daisy chain need control port IP addresses in the same subnet.

Using the command line

You set the IP address by using the **IPA** command. You must have super-user or configuration privileges. The changed IP address takes effect only after you have logged out.

The command syntax is:

IPA:*p*, *ipa*

p	Options are **E**, **C**, and **D**. **C** assigns the IP address to the control port interface for SLIP or PPP, and to the local unit for data link communications; **E** assigns the IP address to the Ethernet interface; and **D** assigns the IP address for data link communications. The use of D depends on the way you have set **NETIF**. When NETIF is set to SD, ED, ESD, or PSD, then IPA:D designates the **remote** unit's data link IP address. When NETIF is D alone, then IPA:D designates the data link IP address of the **local** unit that you are currently configuring. When NETIF is set to any value that does not include D, do not set a data link IP address.
ipa	Enter the IP address using the format *nnn.nnn.nnn.nnn*, where *nnn* can be any number from 0 to 255, inclusive. An IP address of 0.0.0.0 is not valid.

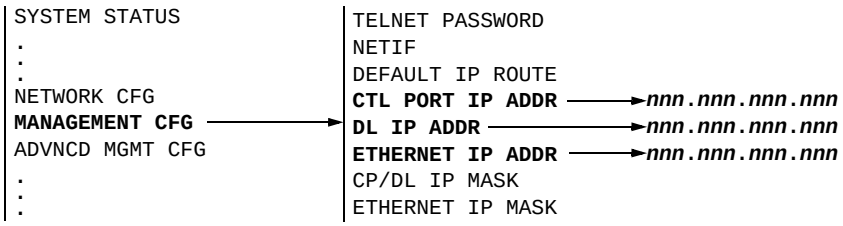
When communicating via the Ethernet interface, you need to assign the controller an Ethernet IP address and a serial port IP address (for communicating to other units in the shelf or daisy-chain via SLIP). The two IP addresses must be on different subnets.

When managing a far-end unit over the data link, you need to assign a data link IP address (see definition above). The near-end unit's control port IP address and the far-end unit's data link IP address must be on the same subnet.

All units in a daisy chain need control port IP addresses in the same subnet.

Using the front panel

The changed IP address takes effect immediately upon pushing Select. To set the desired IP address from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until MANAGEMENT CFG appears in the display.
3. Push Select. TELNET PASSWORD appears in the display.
4. Push Next or Previous until CTL PORT IP ADDR or IN-BAND IP ADDR appears, depending upon which address you want to define.
5. Push Select. The current IP address appears in the display.
6. Push Next or Previous to move between the four fields of the IP address. When the field you want has its first character underlined, push Select.
7. Push Next or Previous to increment or decrement the value. When the value of the field is what you want, push Select.
8. If the entire IP address is correct, push Escape. You will be prompted with: "SET NEW ADDRESS?". Push Select to set the IP address or push Escape to abort.

Setting the IP netmask

The DataSMART unit uses the IP netmask to determine if IP traffic is destined for a host on the same IP network as itself. If the traffic is destined for its network, the unit can send it directly to the host. If the IP traffic is destined for a different network, the unit sends it to the IP address of its default router.

For example, a DataSMART will use the IP netmask to determine whether an incoming packet is addressed to another DataSMART in its IP network, and, if so, accept that packet even if the other DataSMART isn't directly connected to it.

The control port and data link use the same IP netmask. You change this netmask with the **C** parameter of the IPM command or by selecting CP/DL IP MASK from the front panel. Use this netmask for all IP interfaces that use the control port or data link (PPP-SLIP, SLIP, ETH-SLIP, DL, ETH-DL, E-SLIP-DL, P-SLIP-DL, or SLIP-DL).

If your IP interfaces includes Ethernet (ETHERNET, ETH-SLIP, ETH-DL, or E-SLIP-DL), you need to set the Ethernet netmask.

The default IP netmask is 255.255.255.0. Changes to the IP netmask take effect upon logout.

Using the command line

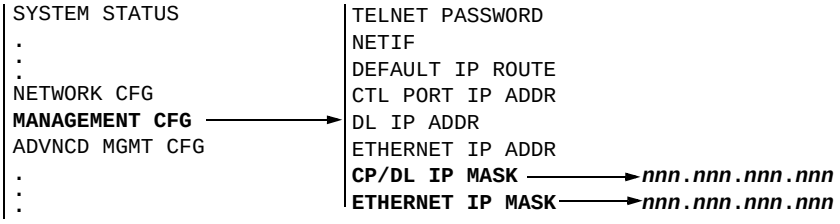
You set the IP netmask by using the **IPM** command. You must have super-user or configuration privileges. The command syntax is:

IPM:*c*, *mask*

c	**C** assigns the IP netmask to the control port and data link interface. **E** assigns the IP netmask to the Ethernet interface.
mask	The IP netmask. It takes the form *nnn.nnn.nnn.nnn*, where *nnn* can be any number from 0 to 255, inclusive. The default is 255.255.255.0.

Using the front panel

To set the IP netmasks from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until MANAGEMENT CFG appears in the display.
3. Push Select. TELNET PASSWORD appears in the display.
4. Push Next or Previous until CTL PORT IP MASK or ETHERNET IP MASK appears, depending upon which netmask you want to define.
5. Push Select. The current IP netmask appears in the display.
6. Push Next or Previous to move between the four fields of the IP netmask. When the field you want has its first character underlined, push Select.
7. Push Next or Previous to increment or decrement the value. When the value of the field is what you want, push Select.
8. If the entire IP netmask is correct, push Escape. You will be prompted with: "SET NEW ADDRESS?". Push Select to set the IP netmask or push Escape to abort.

Setting the Telnet password

The DataSMART Telnet server is enabled and disabled via the Telnet password. A null password (i.e. “”, string length of zero) disables Telnet. Any non-null string enables Telnet. The Telnet password can be up to 15 characters long.

To access the unit via Telnet, the Telnet password must be a non-null string and the IP network interface must be enabled and configured properly.

Using the command line

You set the Telnet password using the **TPW** command. The syntax for the command is shown below. You must have super-user privileges.

TPW:*str*

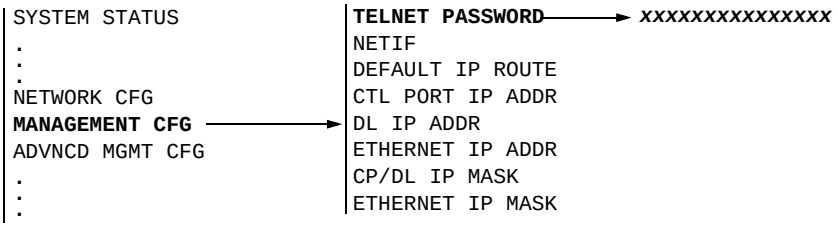
str	Enter the Telnet password. The password can be up to 15 characters long including spaces. Spaces are not allowed at the beginning of the password, but they are allowed in the middle of the password. Trailing spaces are not truncated.

Using the front panel

The operation of the front panel for this command is different than most other commands. The display is not dynamic. The Telnet password will not be changed until the very end when you confirm the change. In addition, if someone on the control port changes the Telnet password, the change will not be reflected on the front panel.

Spaces are allowed at the beginning and in the middle of the password when entered from the front panel.

To set the Telnet password from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until MANAGEMENT CFG appears in the display.
3. Push Select. TELNET PASSWORD appears in the display.
4. Push Select. The current Telnet password appears in the display.
5. Push Next or Previous to move between the fifteen possible characters of the Telnet password. When the character you want is underlined, push Select.
6. Push Next or Previous to increment or decrement the value. When the value of the character field is what you want, push Select.
7. If the entire Telnet password is correct, push Escape. You will be prompted with: “SET NEW STRING?”. Push Select to set the IP address or push Escape to abort.

Selecting the default route IP address

Hosts that are on the same IP network can send IP traffic to each other directly. If a host wants to send IP traffic to a host that is not on the same network, the traffic must be sent to a router that understands the topography of the network. The DataSMART needs to know the address of its default router in order to send packets to another network. This could occur if an SNMP management station is on a different network and is trying to retrieve information from a DataSMART unit.

If a packet is destined for a different network, the unit sends the packet to the IP address of its default router. If there is no default router defined, or if the definition is invalid, the unit discards the packet.

In order for the default router to send a packet to the proper network, you have to configure the default router's static route table. If the default router isn't connected directly to the host, the default router has to link the host address with a forwarding address that will accept the packet and forward it to the host.

The static route table can also be used to forward packets to a DataSMART unit that does not have its own Ethernet IP address. In that case, the unit's control port or data link IP address must be linked in the table with the controller's Ethernet address.

NOTE
You should always set the address of the default router. If a default router does not exist and a DataSMART unit tries to send a packet to a host not on its subnet, the packet will be discarded. This is true for Ethernet, data link, PPP, and SLIP connections.

The default value for the default router address is 192.0.2.2.

For a far-end unit accessing the IP network over the data link, the default router is the near-end DataSMART unit.

Using the command line

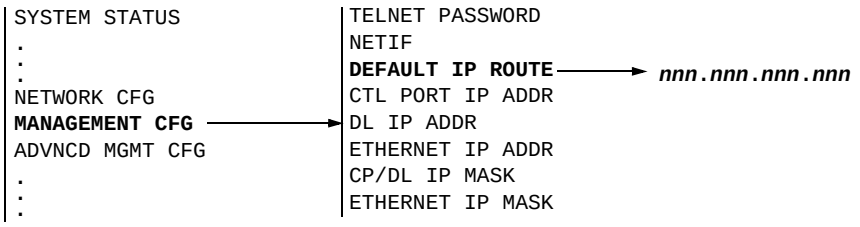
You must have super-user or configuration privileges. The command syntax is:

IPR:*ipa*

ipa	Enter the IP address using the format *nnn.nnn.nnn.nnn*, where *nnn* can be any number from 0 to 255, inclusive. An IP address of 0.0.0.0 is not valid.

Using the front panel

The changed default IP router address takes effect immediately upon pushing Select. To set the desired IP address from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until MANAGEMENT CFG appears in the display.
3. Push Select. TELNET PASSWORD appears in the display.
4. Push Next or Previous until DEFAULT IP ROUTE appears in the display.
5. Push Select. The current IP address appears in the display.
6. Push Next or Previous to move between the four fields of the IP address. When the field you want has its first character underlined, push Select.
7. Push Next or Previous to increment or decrement the value. When the value of the field is what you want, push Select.
8. If the entire IP address is correct, push Escape. You will be prompted with: "SET NEW ADDRESS?". Push Select to set the IP address or push Escape to abort.

Setting up IP source address screening

DataSMART units can screen IP packets based on the source IP address. This security feature lets you screen out packets from any host that is not supposed to access the unit.

For instance, if you know that only network managers should access the DataSMART, you can add their host addresses to the IP screening list and then lock out all other hosts by enabling IP source address screening.

All source address screening commands (the commands discussed in the rest of this section) are found in the Advanced Management Configuration (AMC) menu.

Adding an address or netmask to the IP screening list

Before you can enable IP screening, you must have at least one IP address in the screening list. You can have up to ten addresses total. This list cannot contain multiple entries of the same address, unlike the SNMP trap host list. This list is empty at first power-up.

Adding a netmask to the IP screening list allows you to receive IP packets from any host on the same subnet as the IP address you specify.

Using the command line

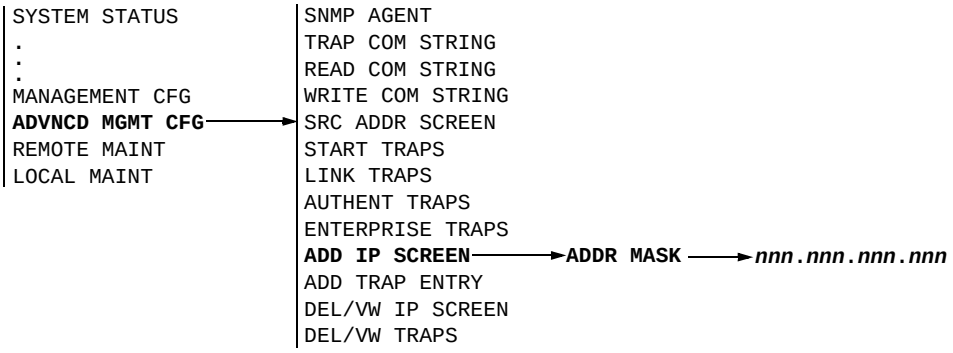
You add an IP address to the IP screening list by using the **ADD** command. You must have super-user or configuration privileges. The command syntax is:

ADD:I:*ipa*[,*mask*]

I	Specify IP source address screening.
ipa	Add the specified IP address to the list.
mask	Use this netmask to define the subnet the specified IP address belongs to, and accept IP packets from any host in that subnet. See "Setting the IP address" on page 179 and "Setting the IP netmask" on page 180 for a detailed description of the *ipa* and *mask* fields.

Using the front panel

To add an IP address or netmask to the IP screening list from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until ADVNCD MGMT CFG appears in the display.
3. Push Select. SNMP AGENT appears in the display.
4. Push Next or Previous until ADD IP SCREEN appears in the display.
5. Push Select. ADDR MASK appears in the display.
6. Push Next or Previous to switch between ADDR and MASK, depending on what you want to change. Then push Select.
7. A blank IP address (000.000.000.000) appears in the display.
8. Push Next or Previous to move between the four fields of the IP address. When the field you want has its first character underlined, push Select. The field blinks.
9. Push Next or Previous to increment or decrement the value. When the value of the field is what you want, push Select.
10. If the entire IP address is correct, push Escape. You will be prompted with: “SET NEW SCREEN?”. Push Select to set the IP address or push Escape to abort.

Viewing and deleting an address from the IP screening list

To delete an address from the IP screening list, source address screening must be disabled. Enabling or disabling source address screening does not take effect until you log out and log back in.

Using the command line

You delete an address from the IP screening list by using the **DEL** command. You must have super-user or configuration privileges. The command syntax is:

DEL:I:*ipa*

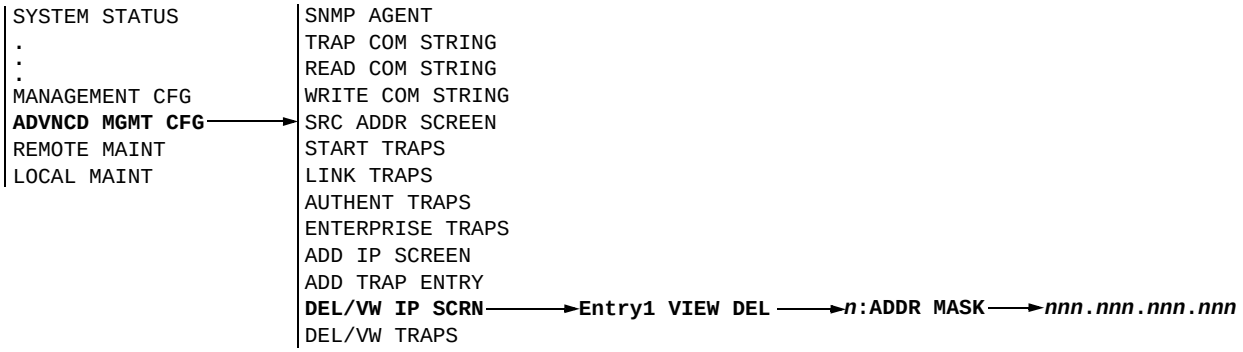
I	Specify IP source address screening.
ipa	Delete the specified SNMP manager's IP address from the list. See "Setting the IP address" on page 179 for a detailed description of the *ipa* field.

or

DEL:I:*	Delete all entries in the list by using the * wildcard.

Using the front panel

To view an IP address in the IP screening list or remove the address from the list with the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until ADVNCD MGMT CFG appears in the display.
3. Push Select. SNMP AGENT appears in the display.
4. Push Next or Previous until DEL/VW IP SCRN appears in the display.
5. Push Select. Entry1 VIEW DEL appears in the display.
6. If you want to select a different entry number, push Select. The entry number is then underlined. Push Next or Previous until you see the number of the entry you want to view, then push Select.
7. Push Next or Previous until VIEW is highlighted.
8. Push Select. *n*: ADDR MASK appears in the display.
9. Push Next or Previous to switch between ADDR and MASK, depending on what you want to view. Then push Select. The IP address appears in the display.

10 Push Select. *n*: ADDR MASK appears in the display.

11 Push Escape. Entry*n* VIEW DEL appears in the display.

12 To delete the entry, push Next or Previous until DEL is highlighted, then push Select. "ADDRESS DELETED" appears in the display.

Enabling and disabling IP source address screening

You can enable IP source address screening after filling in the IP addresses allowed access to the DataSMART.

The default is address screening disabled.

Using the command line

You set the IP Source Address Screening using the **SSA** command. You must have super-user or configuration privileges. The command syntax is:

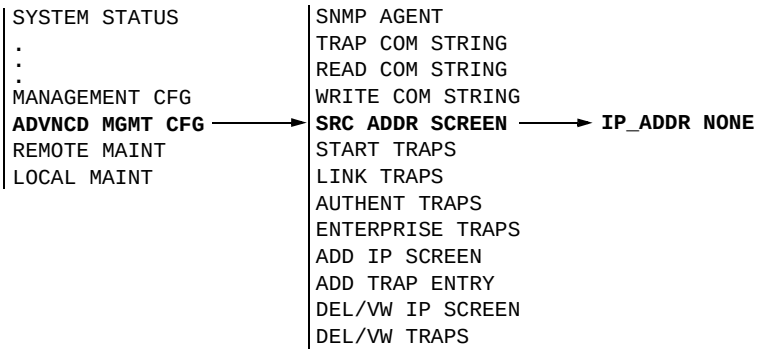
SSA:*c*

The *c* parameter specifies the address screening.

I	Screen based on IP source addresses.
N	No IP address screening.

Using the front panel

To enable or disable IP source address screening from the front panel, use these steps.



1 Push Escape until SYSTEM STATUS appears in the display.

2 Push Next or Previous until ADVNCD MGMT CFG appears in the display.

3 Push Select, then push Next until SRC ADDR SCREEN appears in the display.

4 Push Select. The current state of IP screening appears in the display.

5 Push Next or Previous to move between IP_ADDR and NONE. When the value you want is displayed, push Select.

Configuring for SNMP

To enable the SNMP management capabilities of the DataSMART, the following parameters must be set:

- Enable the SNMP Agent.
- Set the SNMP community strings, if necessary.
- Add the management hosts to the trap list.

NOTE
This section assumes you have already set up the DataSMART for an IP network. This includes: setting the IP address and netmask and selecting the network interface.

Enabling and disabling the SNMP agent

The DataSMART has a fully functional internal SNMP agent. This agent supports MIB II, the DS1 MIB (RFC 1406), and a subset of the Frame Relay DTE MIB (RFC 1315) circuit table as well as link-up, link-down, warm-start, and cold-start traps. The agent also fully supports its own Enterprise MIB.

The IP network interface must be configured since SNMP only works over IP networks.

A warm-start trap is generated by the unit whenever you transition its SNMP agent from disabled to enabled. Enabling the SNMP agent also enables Telnet and the ping response. Enabling or disabling the SNMP agent does not affect automatic FPING generation or FPING tests.

The agent is disabled by default.

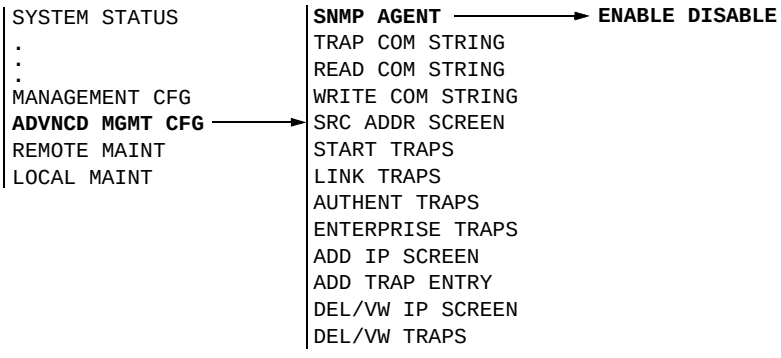
Using the command line

You enable and disable the SNMP agent by using the **ESNMP** and **DSNMP** commands, respectively. You must have super-user or configuration privileges.

ESNMP	Enable the SNMP agent.
DSNMP	Disable the SNMP agent.

Using the front panel

To enable or disable the SNMP agent from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until ADVNCD MGMT CFG appears in the display.

3 Push Select. SNMP AGENT appears in the display.

4 Push Select. The current state of the SNMP agent appears in the display.

5 Push Next or Previous to move between ENABLE and DISABLE. When the value you want is displayed, push Select.

Setting SNMP community strings

There are three SNMP community strings: read, write, and trap. The community strings are another form of (loose) security. If you want to prevent just any SNMP manager from retrieving data from the SNMP agent, you can change the read community string.

Read community string

The read community string controls who can read data from the agent. The default value is “public”.

Write community string

The write community string controls who can write data to the agent using SNMP Sets. The default value is “private”.

Trap community string

The trap community string controls who can read a trap sent from the agent. The default value is “snmptrap”.

Using the command line

You set the SNMP community strings by using the **RCS, WCS,** and **TCS** commands. You must have super-user or configuration privileges. The command syntax is shown below. The strings are allowed to have spaces in them, but you probably won’t want any as other management stations may not allow spaces in community strings.

RCS:*str*

WCS:*str*

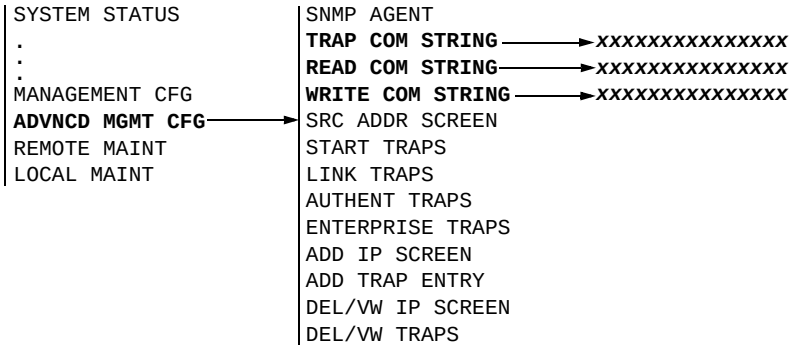
TCS:*str*

where *str* is 1 to 15 characters.

Using the front panel

The operation of the front panel for these commands is different than most other commands. The display is not dynamic. The community string will not be changed until the very end when you confirm the change. In addition, if someone on the control port changes the community string, the change will not be reflected on the front panel.

To set an SNMP community string from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until ADVNCD MGMT CFG appears in the display.
3. Push Select. SNMP AGENT appears in the display.
4. Push Next or Previous until TRAP COM STRING appears in the display. If you want to change the trap community string, proceed to step 5. Otherwise, continue pushing Next or Previous until you see READ COM STRING or WRITE COM STRING, whichever you want to change.
5. Push Select. The current SNMP community string appears in the display.
6. Push Next or Previous to move between the 15 possible characters of the community string. When the character you want is underlined, push Select.
7. Push Next or Previous to increment or decrement the value of the character you want to change. (The front panel display lets you include any printable ASCII character in a community string.) When the character is what you want, push Select.
8. If the entire community string is correct, push Escape. You will be prompted with, "SET NEW STRING?" Push Select to set the community string or push Escape to abort.

Enabling and disabling SNMP traps

DataSMART units can send four kinds of SNMP traps: start, link, authentication, and enterprise. (See "Using SNMP traps" on page 196.) You enable and disable each type of trap separately. All four trap types are enabled by default.

Using the command line

You cannot enable or disable more than one trap type with a single command; for example, to enable start and link traps, you must type

TRAP: E,S
TRAP: E,L

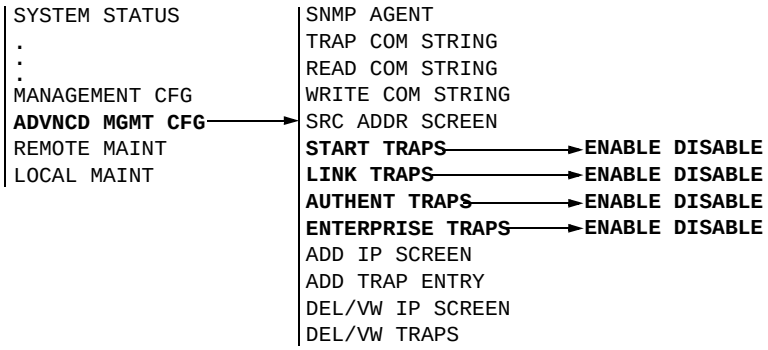
You must have super-user or configuration privileges. The command syntax is:

TRAP:*c,t*

c	Enter **E** to enable the specified traps or **D** to disable them.
t	Specify a trap type to enable or disable: **S** for start, **L** for link, **A** for authentication, and **E** for enterprise.

Using the front panel

To enable or disable SNMP traps from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until ADVNCD MGMT CFG appears in the display.
3. Push Select. SNMP AGENT appears in the display.
4. Push Next or Previous until START TRAPS appears in the display. If you want to enable or disable start traps, proceed to step 5. Otherwise, continue pushing Next or Previous until you see LINK TRAPS, AUTHENT TRAPS, or ENTERPRISE TRAPS, whichever you want to change.
5. Push Select. ENABLE DISABLE appears in the display. The current state is highlighted.
6. Push Next or Previous to move between ENABLE and DISABLE. When the value you want is displayed, push Select.

Configuring the SNMP trap hosts

DataSMART units can send SNMP traps to multiple IP network hosts. In order to send SNMP traps, you must enable the DataSMART SNMP agent (see page 189).

There can be multiple entries of a single address in the SNMP trap list.

Adding an address to the SNMP trap host list

The SNMP trap host list contains the IP addresses of all IP network hosts that you want the DataSMART unit to send traps to. The SNMP trap host list is empty at first power-up. You add an IP address to the SNMP trap list by using the **ADD** command.

If your unit is configured for NETIF=D and the IP management path goes straight to a trap host without communicating through a DataSMART unit, you must associate the path's Data Link Connection Identifier (DLCI) with the trap host's IP address. Your carrier or network administrator should be able to provide the DLCI.

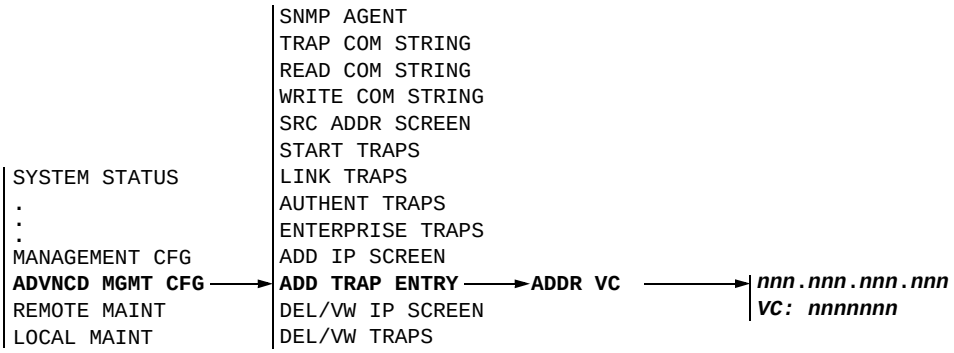
You must have super-user or configuration privileges. The command syntax is:

ADD:T:*ipa*[,*dlci*]

T	Specify SNMP trap list.
ipa	Add the specified IP address to the list. See "Setting the IP address" on page 179 and "Setting the IP net-mask" on page 180 for a description of the *ipa* and *mask* fields.
dlci	Enter the DLCI associated with the trap host's IP address.

Using the front panel

To add an IP address to the SNMP trap list from the front panel, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until MANAGEMENT CFG appears in the display.
3. Push Select. Push Next or Previous until ADD TRAP ENTRY appears in the display.
4. Push Select. ADDR VC appears in the display. ADDR is blinking.
5. Push Select. An IP address of 0.0.0.0 appears.
6. Push Next or Previous to move between the four groups of the IP address. When the group you want has its first character underlined, push Select.
7. Push Next or Previous to increment or decrement the value. When the value is what you want, push Select.
8. Push Escape. ADDR VC appears in the display again.
9. Push Next or Previous until VC is blinking, then push Select. A VC appears.

10 Push Next or Previous to increment or decrement the value. When the value is what you want, push Select.

Viewing and deleting an address from the SNMP trap list

If there are multiple entries of a single address in the table, each entry must be deleted. One deletion does not clear out all occurrences of that address.

Using the command line

You delete an address from the SNMP trap list by using the **DEL** command. The syntax for the command is shown below. You must have super-user or configuration privileges.

DEL:T:*ipa*

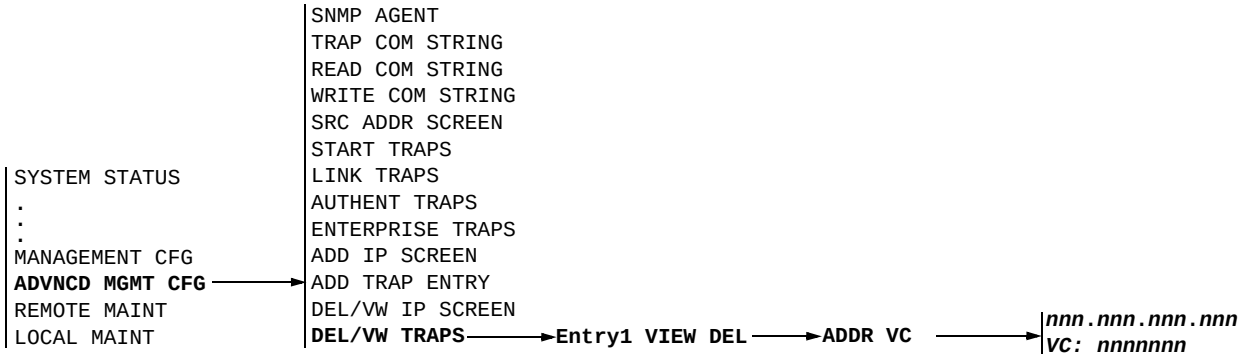
T	Specify SNMP trap list.
ipa	Delete the specified SNMP manager's IP address from the list. See "Setting the IP address" on page 179 for a detailed description of the *ipa* field.

or

DEL:T:*	Delete all entries in the list by using the * wildcard character.

Using the front panel

To view or delete an IP address from the SNMP trap list, use these steps.



1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until ADVNCD MGMT CFG appears in the display.
3. Push Select. SNMP AGENT appears in the display.
4. Push Next or Previous until DEL/VW TRAPS appears in the display.
5. Push Select. Entry1 VIEW DEL appears in the display.
6. If you want to select a different entry number, push Select. The entry number is then underlined. Push Next or Previous until you see the number of the entry you want to view, then push Select.
7. Push Next or Previous until VIEW is highlighted.
8. Push Select. *n*: ADDR VC appears in the display.
9. Push Next or Previous to switch between ADDR and VC, depending on what you want to view. Then push Select. The item you selected appears in the display.
10. Push Select. *n*: ADDR VC appears in the display.
11. Push Escape. Entry*n* VIEW DEL appears in the display.
12. To delete the entry, push Next or Previous until DEL is highlighted, then push Select. “ADDRESS DELETED” appears in the display.

Using SNMP traps

SNMP traps are like DataSMART alarm messages: they indicate alarm conditions in the network.

Configuration for SNMP traps

To use SNMP traps, you must:

- Connect the DataSMART to a TCP/IP network, either in-band or over a SLIP or PPP connection on the control port.
- Enable the DataSMART SNMP agent by using the **ESNMP** command (see page 189).
- Enable any combination of start, link, authentication, and enterprise-specific traps.

SNMP traps also need a destination IP address. You have ten possible trap destinations defined by the trap host list (see "Configuring for SNMP" on page 189). At the trap host destination there must be an SNMP network management application. These programs understand SNMP and can interact intelligently with the DataSMART SNMP agent.

Types of SNMP traps

DataSMART units can generate these trap types:

Start traps:

- Warm-start
- Cold-start

Link traps:

- Link-down
- Link-up

Authentication traps:

- Telnet Password
- SNMP Rd CommString
- SNMP Wr CommString
- IP Screen

Enterprise traps:

- Excessive Error Rate (EER)

Warm-start trap

The warm-start trap is generated every time you enter **ESNMP** (enable SNMP) from the command line and the agent was previously disabled.

Cold-start trap

The cold-start trap is generated every time the DataSMART is power-cycled. Cold-start traps are not generated until ten seconds after the unit is power-cycled. This allows time for the hardware providing the low-level IP network interface to start up and stabilize before attempting to send a packet.

Link-down trap

A link-down trap is generated when *ifOperStatus* (MIB II) changes to *down*.

Link-up trap

A link-up trap is generated when *ifOperStatus* (MIB II) changes to *up*.

Telnet Password

A Telnet Password trap is generated when an incorrect Telnet password has been entered.

SNMP Rd CommString

A SNMP Rd CommString trap is generated when the DataSMART has read an incorrect SNMP community string.

SNMP Wr CommString

A SNMP Wr CommString trap is generated when the DataSMART has written an incorrect SNMP community string.

IP Screen

An IP Screen trap is generated when the DataSMART has received a trap or message from a device whose IP address is not on the Source Screening Address list.

NOTE
The events that generate the Telnet Password, SNMP Rd CommString, SNMP Wr CommString, and IP Screen traps are also logged in the Security History report (see "Interpreting the Security History report" on page 127).

Excessive Error Rate

An Excessive Error Rate trap is generated whenever the Excessive Error Rate threshold is exceeded (see "Specifying the error threshold evaluation window" on page 66).

MIB objects included in SNMP traps

SNMP allows any MIB object to be included in a trap. The DataSMART includes information on its status and that of the T1 line, to speed analysis. Each trap type includes different information.

Warm-start trap

A warm-start trap includes the *ifDescr* and *ifIndex* of all interfaces on the unit.

Cold-start trap

A cold-start trap includes the *ifDescr* and *ifIndex* of all interfaces on the unit.

Link-down trap for a T1 interface

A link-down trap for a T1 interface includes the following:

- *ifDescr*—"T1 Network Interface"
- *ifIndex*—this is the instance number for that interface
- *dsx1LineStatus*—a bitmap of the T1 line's current state
- *dsx1CurrentESs*—the number of errored seconds for the current interval
- *dsx1CurrentUASs*—the number of unavailable seconds for the current interval

Link-up trap for a T1 interface

A link-up trap for a T1 interface includes the following:

- *ifDescr*—"T1 Network Interface"
- *ifIndex*—this is the instance number for that interface
- *dsx1LineStatus*—a bitmap of the T1 line's current state
- *dsx1CurrentESs*—the number of errored seconds for the current interval
- *dsx1CurrentUASs*—the number of unavailable seconds for the current interval

Telnet Password authentication trap

The Telnet Password trap includes the following:

- *dsRpShrDateTime*—the date and time the event occurred
- *dsRpShrEventType*—"rpShrTelnetPassword" (Type 1)
- *dsRpShrComments*—the source IP address of the unit that sent the incorrect Telnet password

SNMP IP Screen authentication trap

The SNMP IP Screen trap includes the following:

- *dsRpShrDateTime*—the date and time the event occurred
- *dsRpShrEventType*—"rpShrSrcIpAddressScreen" (Type 2)
- *dsRpShrComments*—the source IP address of the device that sent the message to the M-PATH unit

SNMP Rd CommString authentication trap

The SNMP Rd CommString trap includes the following:

- *dsRpShrDateTime*—the date and time the event occurred
- *dsRpShrEventType*—"rpShrReadCommString" (Type 3)
- *dsRpShrComments*—the source IP address of the unit that caused the event

SNMP Wr CommString authentication trap

The SNMP Wr CommString trap includes the following:

- *dsRpShrDateTime*—the date and time the event occurred
- *dsRpShrEventType*—"rpShrWriteCommString" (Type 4)
- *dsRpShrComments*—the source IP address of the unit that caused the event

Set NI Excessive Error Rate enterprise trap

The Set NI Excessive Error Rate trap includes the following:

- *ifDescr*—"Set NI Excessive Error Rate (NEER)"
- *ifIndex*—this is the instance number for the network interface
- *dsx1LineStatus*—a bitmap of the T1 line's current state
- *dsx1CurrentESs*—the number of errored seconds for the current interval
- *dsx1CurrentUASs*—the number of unavailable seconds for the current interval

Clear NI Excessive Error Rate enterprise trap

The Clear NI Excessive Error Rate trap includes the following:

- *ifDescr*—"Clear NI Excessive Error Rate (NEER)"
- *ifIndex*—this is the instance number for the network interface
- *dsx1LineStatus*—a bitmap of the T1 line's current state
- *dsx1CurrentESs*—the number of errored seconds for the current interval
- *dsx1CurrentUASs*—the number of unavailable seconds for the current interval

Set TI Excessive Error Rate enterprise trap

The Set TI Excessive Error Rate trap includes the following:

- *ifDescr*—"Set TI Excessive Error Rate (NEER)"
- *ifIndex*—this is the instance number for the terminal interface
- *dsx1LineStatus*—a bitmap of the T1 line's current state
- *dsx1CurrentESs*—the number of errored seconds for the current interval
- *dsx1CurrentUASs*—the number of unavailable seconds for the current interval

Clear TI Excessive Error Rate enterprise trap

The Clear TI Excessive Error Rate trap includes the following:

- *ifDescr*—"Clear TI Excessive Error Rate (NEER)"
- *ifIndex*—this is the instance number for the terminal interface
- *dsx1LineStatus*—a bitmap of the T1 line's current state
- *dsx1CurrentESs*—the number of errored seconds for the current interval
- *dsx1CurrentUASs*—the number of unavailable seconds for the current interval

Traps and alarm conditions

The following table correlates alarm conditions to traps.

Alarm Condition	Trap
ECF	Link down on network interface
NI LOS	Link down on network interface
NI OOF	Link down on network interface
NI AIS	Link down on network interface
NI YEL	Link down on network interface
NI EER	EER enterprise trap on network interface
TI LOS	Link down on terminal interface
TI OOF	Link down on terminal interface
TI AIS	Link down on terminal interface
TI YEL	Link down on terminal interface
TI EER	EER enterprise trap on terminal interface
DP LOS	Link down on data port
Agent-enabled	Warm-start trap
Power-up	Cold-start trap

CHAPTER

9 Quick reference

This chapter contains:

- A listing of all menus and commands available through the command-line interface
- A flowchart of all menus and commands available through the front-panel interface
- A summary of commands accessible through an **ARC** login
- A description of how the DataSMART generates T1 alarms, based on signal conditions at the network interface
- A complete listing of the DataSMART specifications

Command-line menus and commands

The command-line interface provides eighteen “help” menus. These menus group the various commands by function and describe the use and syntax of each command.

To display a menu, simply enter the one- or two-letter acronym for the menu title.

Main menu (MM)

```
DataSMART 6nn Version 1.nn Copyright (c) 1996-97 Kentrox
        ADDRESS: 00:00:000      NAME: PORTLAND,OR

MM                      - Main Menu
SS                      - System Status and Remote Menu
R                       - Reports Menu

LM                      - Local Maintenance Menu
RM                      - Remote Maintenance Menu

AC                      - Alarm Configuration Menu
CC                      - Control Port Configuration Menu
DC                      - Data Port Configuration Menu
FC                      - Fractional T1 Configuration Menu
MC                      - Management Configuration Menu
NC                      - NI Configuration Menu
PC                      - Password Entry and Configuration Menu
SC                      - System Configuration Menu
TC                      - TI Configuration Menu

^D                      - Logout
^D<xx>:<yy>:<zzz>^E     - Address Another Unit

MM>
```

System Status and Remote menu (SS)

```
                SYSTEM STATUS AND REMOTE MENU

ARC/DRC         - Access to/Disconnect from Remote Unit Control
S               - System Status Screen Command

SSV             - View System Setup
```

Reports menu (R)

```
                 REPORTS MENU

UNSR / UNLR     - User NI Short/Long Performance Report
UTSR / UTLR     - User TI Short/Long Performance Report
CNSR / CNLR     - Carrier NI Short/Long Performance Report
FESR / FELR     - Far End PRM Short/Long Performance Report

NSR:[z]         - User NI Statistical Performance Report
TSR:[z]         - User TI Statistical Performance Report
                  z = Display Report then Zero Counts (Optional)
AHR             - Alarm History Report
SHR             - Security History Report

PL:<len|style>  - Set Page Length, <len> = 20 .. 70 (or 0 = Off), or
                  <style> = P (Page Break), M (More), or V (View)
```

add/drop only — UNSR / UNLR, UTSR / UTLR, CNSR / CNLR, FESR / FELR

add/drop only — NSR:[z], TSR:[z]

Local Maintenance menu (LM)

```
                LOCAL MAINTENANCE MENU

SLL     - Set Line Loop Back
SPL     - Set Payload Loop Back
SLO     - Set Local Loop Back
STI     - Set TI Loop Back
SDP<n>  - Set Data Port Loop Back at Data Port, n=1
SDT<n>  - Set Data Terminal Loop Back at Data Port, n=1
RLB     - Reset Loop Backs

DST    - Do Self Test
```

add/drop only

Remote Maintenance menu (RM)

```
                REMOTE MAINTENANCE MENU

SRL             - Set Remote Line Loop Back
SRP             - Set Remote Payload Loop Back
SRDP<n>         - Set Remote Data Port Loop Back, n = 1
RST1            - Reset Remote Loop Back

SQC/S3C/S1C/S0C - Send Test Codes at NI: QRS, 3/24, 1 ,0
S5C<n>          - Send 511 Test Code in Data Port <n> Bit Stream
S2C<n>          - Send 2047 Test Code in Data Port <n> Bit Stream
RTC             - Reset Test Codes

BTQ/BT3/BT1/BT0 - Activate BERT using Test Codes: QRS, 3/24, 1 ,0
BT5<n>          - Activate BERT using 511 at Data Port n = 1
BT2<n>          - Activate BERT using 2047 at Data Port n = 1
```

Alarm Configuration menu (AC)

```
                ALARM CONFIGURATION MENU

EAM / DAM       - Enable/Disable Alarm Messages

EYL / DYL       - Enable/Disable YELLOW Activating an Alarm
DACT:<n>        - Alarm Deactivation time in seconds, n = 1..15
EST:<n>         - Errored Second Threshold, n = 0 .. 900
UST:<n>         - Unavailable Second Threshold, n = 0 .. 900
ST15/ ST60      - Set Threshold Timing to 15 or 60 Minutes


ACV             - View Alarm Configuration
```

Control Port Configuration menu (CC)

```
                CONTROL PORT CONFIGURATION MENU

EE / DE - Enable/Disable Character Echo

DCE/DTE - Select the Control Port

CCV     - View Control Port Configuration
```

Data Port Configuration menu (DC)

```
                DATA PORT CONFIGURATION MENU

EDI<n> / DDI<n> - Enable/Disable Data Inversion at Data Port, n=1
SCLK<n>:<clk>   - Source Clock at Data Port, n=1
                  clk = I (Internal), E (External)
TCLK<n>:<cmd>   - Transmit Clock Inversion at Data Port, n=1
                  cmd = E (Enable), D (Disable)
RCLK<n>:<cmd>   - Receive Clock Inversion at Data Port, n=1
                  cmd = E (Enable), D (Disable)
IDL<n>:<char>   - Idle Character at Data Port, n=1
                  char = 7E (0x7E), 7F (0x7F), FF (0xFF)
DPLOS<n>:<los>  - LOS Input Signal at Data Port, n=1
                  los = R (RTS), D (DTR), B (Both), N (No Processing)

DCV             - View Data Port Configuration
```

Fractional T1 Configuration menu (FC)

```
                FRACTIONAL T1 CONFIGURATION MENU

<table>DP<port>:<rate>[,<nicn>]
                        - DP=Assign NI Channel Map for Data Port
    table A/B           - Tables A or B Containing Channel Assignment
    port  1             - Data Port Number
    rate  56/64         - Channel Rate in 1000 bps
    nicn  1 .. 24       - NI Channel numbers assigned to Data Port
          1,3,5,...     - Can be alternating DS0 channel numbers or
          1-24          - a contiguous range.
```

TI channel assignments available on add/drop units only

```
<table>NI<nicn>:<ticn>,<nicn>:<ticn>, ...
                        - NI=Assign NI Channels to TI or IDLE
    table A/B           - Tables A or B Containing Channel Assignment
    nicn  1 .. 24       - NI Channel numbers
    ticn  V,D,I         - Voice/Data on TI Channel or I for Idle

CPAB / CPBA             - Copy A to B or B to A
LXA  / LXB              - Load and Execute Table A or B
TAV  / TBV              - View Table A or B
TXV                     - View Executing Channel Assignment
```

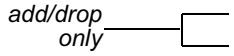
Management Configuration menu (MC)

```
                MANAGEMENT CONFIGURATION MENU

TPW:<str>           - Set Telnet Password, str=0 to 15 characters
                      0 characters disables Telnet
NETIF:<p>[,<dl>[,<spd>]]
                    - Set IP Network Interface Paths
                    <p> = N, E, PS, S, D, ES, ED, ESD, PSD, or SD
                    N = None, E = Ethernet, P = PPP, S = SLIP,
                    D = Datalink  -  if Datalink, use dl and spd
                    <dl> = F (FDL), 1-24 (DS0 Tslot) - if DS0, use spd
                    <spd> = 56 (56k of DS0 Tslot), 64 (All of Tslot)
IPR:<ipa>          - Set Default Route IP Address
IPA:<p>,<ipa>      - Set IP Addresses
IPM:<p>,<mask>     - Set IP Masks
                     p = E (Ether), C (PPP/SLIP), D (Datalink)
                     <ipa> and <mask> = n.n.n.n, n = 0 .. 255 (dec)
                     <ipa> for Datalink is IP Address of remote unit
                     <mask> is the same for Ctl Port and Datalink

AMC                - Advanced Management Configuration Menu
MCV                - View Management Configuration
```

Advanced Management Configuration menu (AMC)

```
              ADVANCED MANAGEMENT CONFIGURATION MENU

ESNMP/DSNMP         - Enable/Disable SNMP Agent

TCS:<str>           - Set SNMP Trap Comm String, str=1 to 15 characters
RCS:<str>           - Set SNMP Read Comm String, str=1 to 15 characters
WCS:<str>           - Set SNMP Write Comm String, str=1 to 15 characters

SSA:<p>             - Set Packet Screening via Source Address
                      p = I (IP Addr), N (None)
TRAP:<c>,<t>        - SNMP Trap Generation c = E (Enable), D (Disable)
                      t = S (Start), L (Link), A (Auth), E (Enterprise)
ADD:T,<ip>[,dlci]   - Add IP Address to Trap Dest List
                      <dlci> = optional identifier for Data Link Traps
ADD:I,<ip>[,mask]   - Add IP Address to Screening List
DEL:<l>,<ip>        - Delete Address from Screening or Trap Dest Lists
                      <l> = I (IP Screen List), T (Trap Dest List)
                      <ip> and [mask] = n.n.n.n, n = 0 .. 255 (dec)
                      [mask] used only for IP Screen List and is optional

AMCV                - View Advanced Management Configuration
```

Network Interface Configuration menu (NC)




```
          NI CONFIGURATION MENU

NSF/NESF/NERC     - NI SF/ESF/Ericsson Framing Format
NAMI / NB8        - NI AMI/B8ZS Line Coding
EPRM / DPRM       - Enable/Disable T1.403 PRM Generation out NI
FKA / UKA         - Framed/Unframed Keep Alive
EYEL / DYEL       - Enable/Disable YELLOW Activation out NI
ADR54:<Trgt>      - 54016 Address = C(CSU), D(DSU), or B(Both)
E54 / D54         - Enable/Disable 54016 Mode

                Line Build Out
NL0                -  0.0 dB
NL1                -  7.5 dB
NL2                - 15.0 dB

NCV                - View NI Configuration
```

Password Entry and Configuration menu (PC)

```
        PASSWORD ENTRY AND CONFIGURATION MENU

EPS:<password>          - Enter Password
                          password = 6 to 12 characters

APS:<access>:<password> - Add Password
                          access   = SA - Super User
                                     CA - Configuration
                                     MA - Maintenance
                          password = 6 to 12 characters

DPS:<password>          - Delete Password
                          password = 6 to 12 characters, or * for all

PUV                     - View User Access Privilege
PCV                     - View Password Configuration
```

System Configuration menu (SC)

```
                SYSTEM CONFIGURATION MENU

 SD:<mm>,<dd>,<yy>        - Set Date (Warning: This also clears reports)
 ST:<hh>,<mm>             - Set Time (Warning: This also clears reports)
 SN:<id>                  - Set Name
 SA:<xx>,<yy>,<zzz>       - Set the Unit's Address to slot:shelf:group
 EFP / DFP                - Enable/Disable Front Panel Operation
 EDC / DDC                - Enable/Disable DataSMART Compatibility
 CLK:<src>                - Clock Source, src = L (Loop), C (CSU Thru)
                            T (TI Receive), I (Internal), 1 (DP1)
 ALGOUT:<n>               - Autologout, n = 0 .. 60 minutes
 ZALL                     - Zero All Counters used in User Reports
 TSWDL:<i>                - Download program from a file via TFTP
                            i = n.n.n.n, n = 0..255 (dec), the
                                IP address of the TFTP host system
 BOOT:<b>                 - Re-boot the system
                            b = A (Active FLASH) or I (Inactive FLASH)
 WYV                      - View "What's Your Version" Information
 RSD                      - Reset System to Default Values
 SCV                      - View System Configuration
```

Terminal Interface Configuration menu (TC)—DataSMART 658 only

```
                  TI CONFIGURATION MENU

TSF/TESF/TERC  - TI SF/ESF/Ericsson Framing Format
TAMI/TB8       - TI AMI/B8ZS TI Line Coding
TIDL:<c>       - Idle Code, c = 00-FF Hex

                  TI Equalization
TE0            -   0 - 133 ft
TE1            - 133 - 266 ft
TE2            - 266 - 399 ft
TE3            - 399 - 533 ft
TE4            - 533 - 655 ft

TCV            - View TI Configuration
```

Front-panel menus and commands

In the flowcharts below, movement through the front-panel interface is denoted as follows:

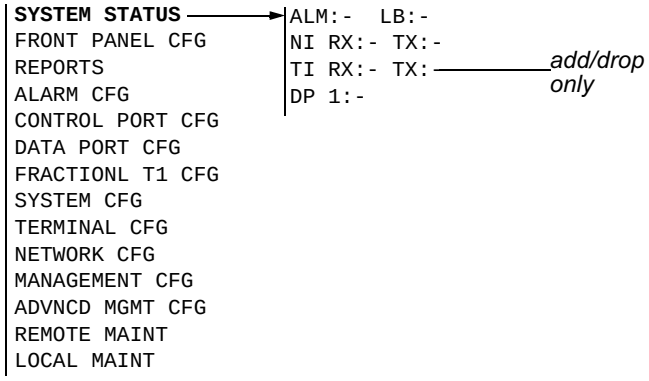
- A vertical line to the left of a column represents a menu listing that you cycle through by pushing the Next or Previous button.
- A vertical line to the right of a column means that each item in the list has the same entry path into the next menu or command (listed to the left).
- An arrow represents a path you enter by pushing the Select button, and exit by pushing the Escape button.
- Bold face type represents a specific path through the interface, starting at the top of the menu hierarchy.

You cycle through command fields by pushing the Next or Previous button. You select field values by pushing the Select button.

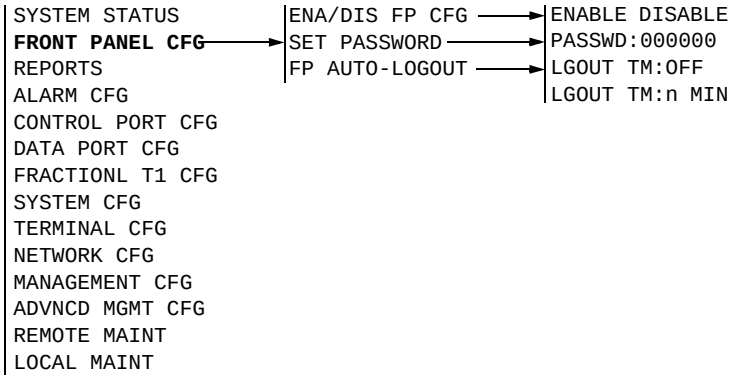
You can always escape to the top menu by pushing the Escape button repeatedly.

If the front-panel is disabled, it defaults to a display of %EFS (percentage error-free seconds).

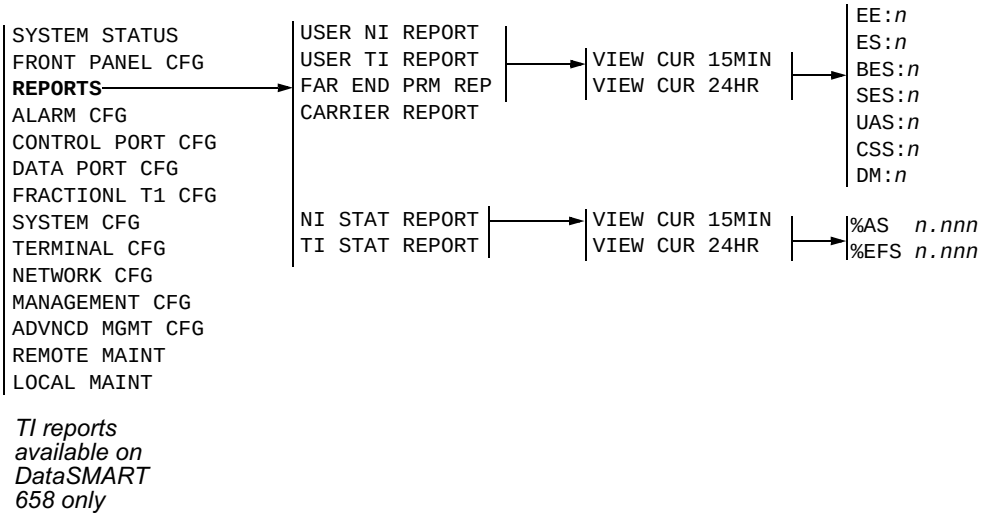
System status



Front-panel configuration

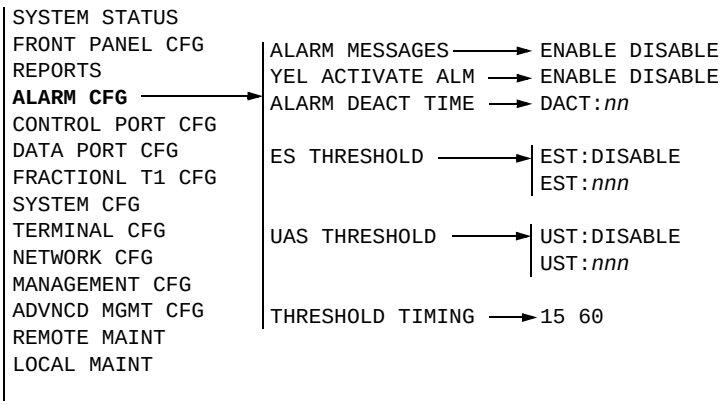


Reports

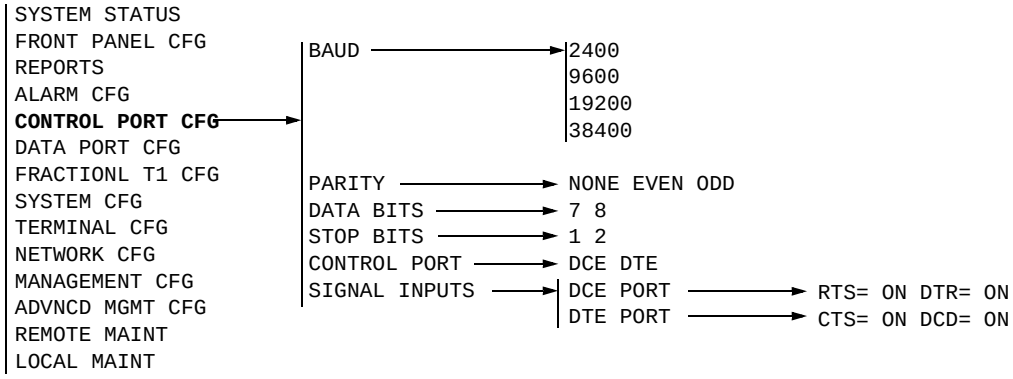


TI reports available on DataSMART 658 only

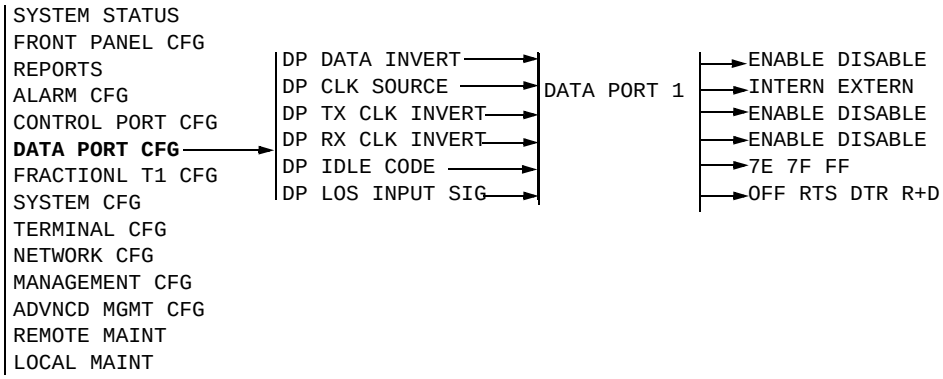
Alarm configuration



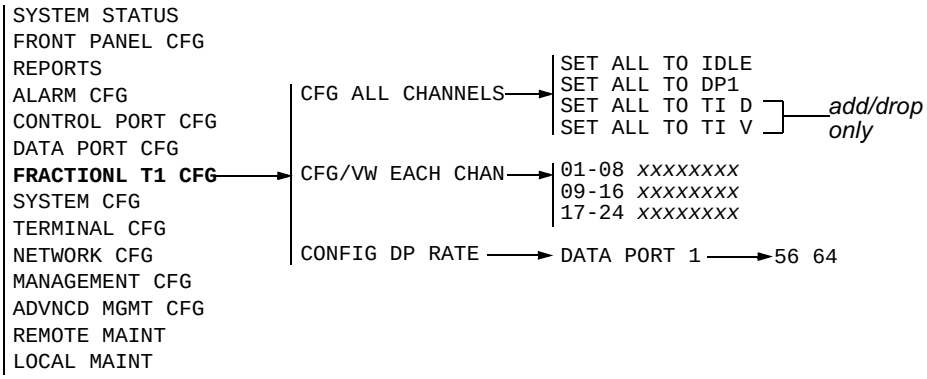
Control port configuration



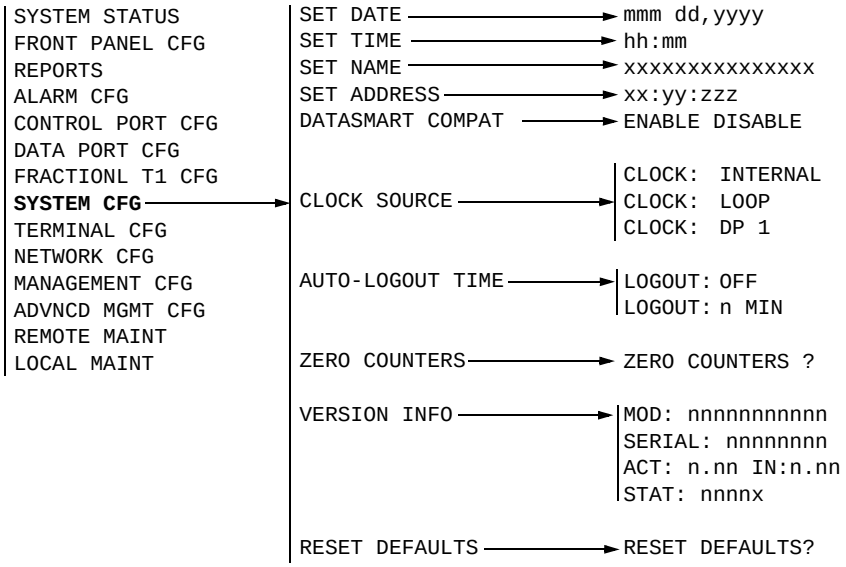
Data port configuration



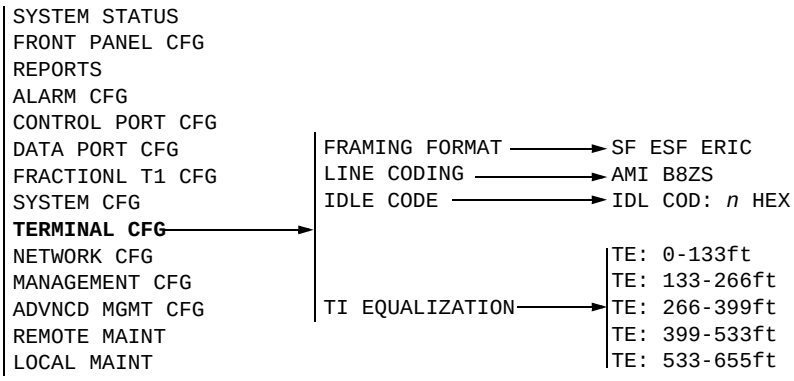
Fractional T1 configuration



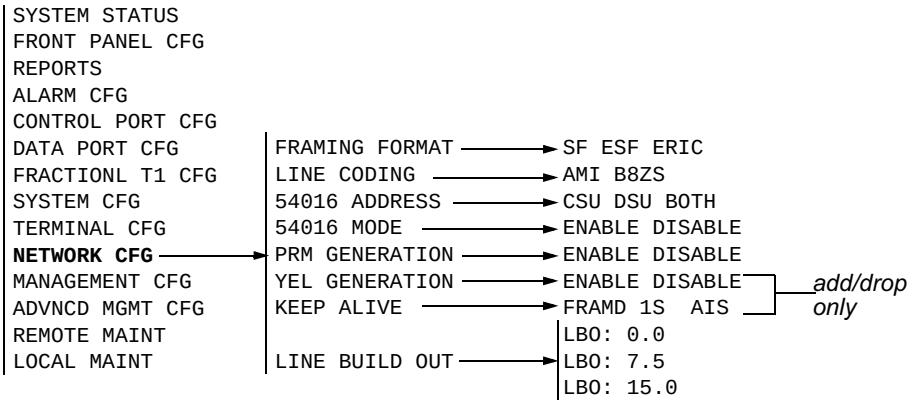
System configuration



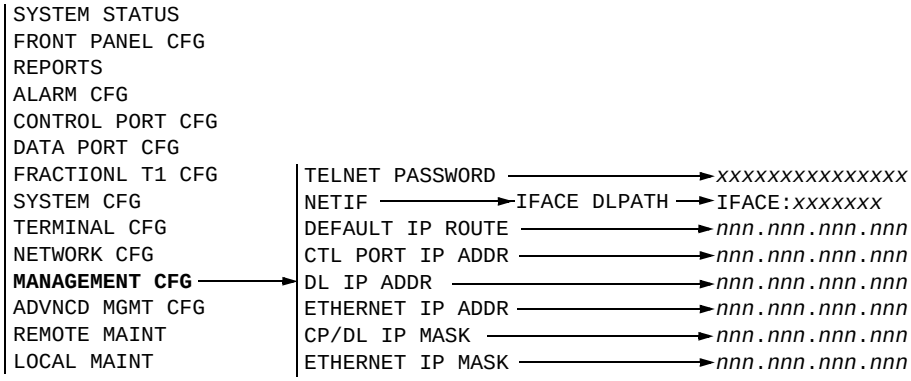
Terminal configuration (DataSMART 658 only)



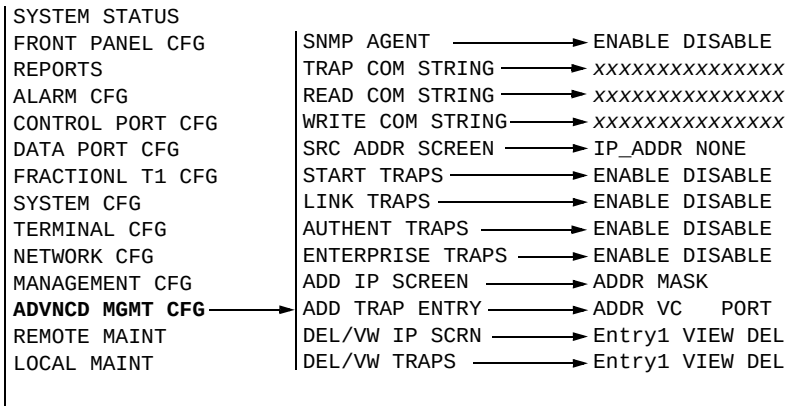
Network configuration



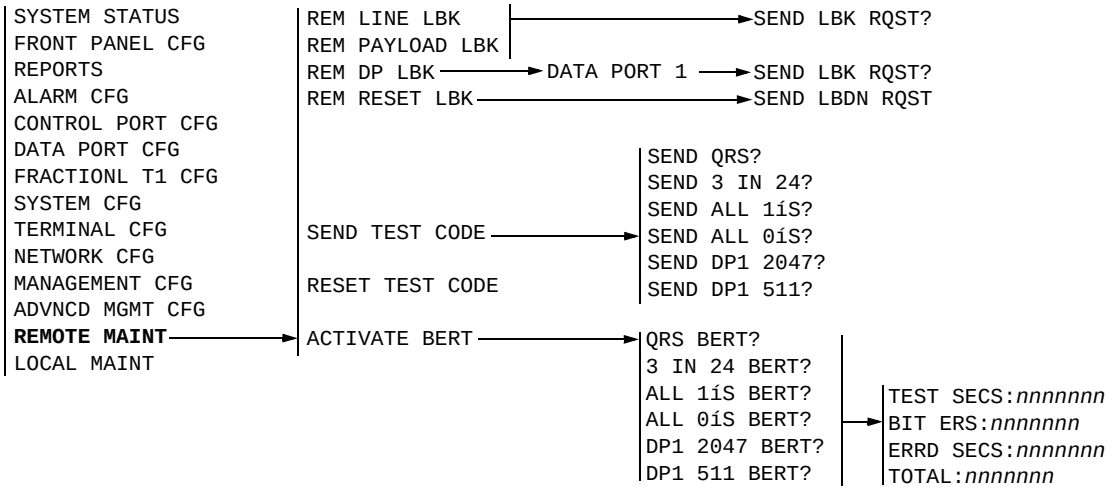
Management configuration



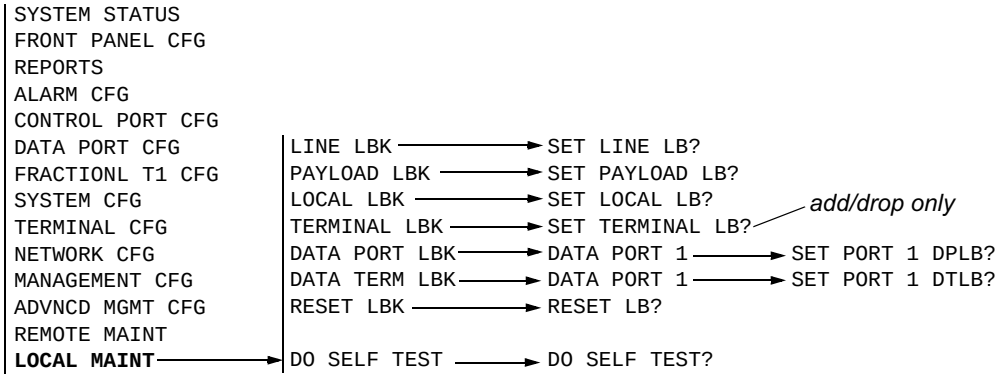
Advanced management configuration



Remote maintenance



Local maintenance



Commands available via ARC

You can log into a remote DataSMART, DataSMART SPort, DataSMART MAX unit, or M-PATH CSU by using the **ARC** command. This command establishes the remote login via the FDL (facility data link) line in the T1 signal. The T1 framing format must be ESF (extended super frame). The **DRC** command disconnects the remote login.

The **ARC** command's actions are affected by the **EDC/DDC** commands. The default power-up value is DataSMART 72000 series compatible, including DataSMART MAX, SPort and M-PATH CSU. No action is required.

EDC (enable DataSMART 78000 series compatibility) command

Use the **EDC** command prior to executing **ARC** to specify that you are connecting to a DataSMART 78000 series DSU/CSU. Executing **EDC** has the following effects:

- Remote data loopbacks: all SRDP data port commands and the next RST1 command following SRDP generate the inverted 127 code in a format compatible with DataSMART. The code is transmitted continuously for 10 seconds or until the loop action is verified.
- T1.403 remote payload loopbacks: if the DataSMART is the remote unit, then the DataSMART does not expect loopback retention codes to be transmitted from the remote unit.

DDC (disable DataSMART 78000 series compatibility) command

Use the **DDC** command to disable DataSMART 78000 series DSU/CSU compatibility and restore **ARC** compatibility with DataSMART 72000 series units, including MAX and SPort, and M-PATH CSU. Executing **DDC** has the following effects:

- Remote data loopbacks: all SRDP commands and the next RST1 command following SRDP generate the code in a format compatible with Annex B of T1.403-1994. The code is transmitted for approximately 2.5 seconds, followed by a transmission of all ones lasting approximately 2.5 seconds. Since the remote unit is required to perform the loop activity within 2 seconds of receiving the all-ones code, the DataSMART sends a momentary loop code again after the 2.5 seconds of all ones to confirm the loop actions. If ten seconds elapse before the loop action is verified, the loop is considered unverified. Setting and resetting remote data port loopbacks may not be reliable if this setting is incorrect.
- T1.403 remote payload loopbacks: the DataSMART expects retention codes as defined in T1.403-1994. If they are not received (as from a DataSMART unit) the unit actuates the loopback and immediately resets it.

Command compatibility

You can access most DataSMART commands via an ARC remote login. The only commands you cannot access are those that could potentially break the FDL link, or those that set up the network interface or the terminal interface. The commands that you cannot access through **ARC** are:

DataSMART menu	Commands *not* accessible via ARC
System Status menu	EDC, DDC
Local Maintenance menu	DST, SDP, SDT, SLL, SLO, SPL, STI
Remote Maintenance menu	BT*t*, SRP, SRL, SRDP, S*t*C, RTC, RST1
NI Configuration menu	NAMI, NB8, NERC, NESF, NL*x*, NSF
System Configuration menu	TSWDL
TI Configuration menu	TAMI, TB8, TERC, TE*n*, TESF, TSF

DataSMART 78000 series DSU compatibility

You can execute only a subset of the commands for the DataSMART 78000 series DSU (older DataSMART models such as the Single-Port and Quad-Port) via an ARC remote login. The subset consists of the commands found on the DataSMART Control Port Configuration menu and on its Status and Remote menu.

DataSMART menu	Commands accessible via ARC	Command functions
System Status and Remote menu	S	System Status Screen command
Fractional T1 Configuration menu	CPA/CPB	Copy A to B or B to A
	LXA/LXB	Load and execute table A or table B
	TAV/TBV	View table A or table B
	TXV	View executing channel assignment
	<table>DP	Assign channels to data port
	<table>NI	Assign channels to terminal or idle

- The FC command returns a DataSMART DC menu from a DataSMART 78000 series DSU and a DataSMART FC menu from the newer DataSMART models (MAX, SPort, 680) and the M-PATH CSU.
- The DC command returns an FC menu from a newer DataSMART model (or M-PATH) and a DC menu from a DataSMART 78000 series DSU.

T1 alarms and signal processing

This section describes how the DataSMART transitions into and out of an alarm state. It also describes in detail the alarms that can occur at the network and terminal T1 interfaces and the signal conditions that cause them.

NOTE
For a complete listing of all alarms generated by the DataSMART and appropriate troubleshooting procedures, refer to Chapter 7, "Troubleshooting".

What happens when alarms occur

When the DataSmart transitions to an alarm state, it performs various actions:

- It illuminates appropriate LEDs on the front panel.
- It updates the System Status display with status information about the alarms and signal conditions at the network interface, terminal interface, and data ports.
- It outputs an SNMP trap or an alarm message to the control device (if traps or messages are enabled) and logs the alarm message in the Alarm History report.
- It transmits yellow alarms and idle code out the interfaces and data ports as appropriate.
- It switches the clock source to internal master timing, if the condition obstructs the clocking source.

How alarms are generated

The DataSMART generates alarms based on error events that occur in an input signal. Error events are also referred to as signal conditions. For instance, a loss of signal event (LOS) is also referred to as an LOS signal condition. A signal condition is a current, instantaneous status of the received signal at the interface. The signal condition may persist, may be intermittent, or may disappear immediately.

If a signal condition persists or is intermittent but frequent, the DataSMART transitions into an alarm state, a process called "alarm integration." The algorithm that controls alarm integration is designed to prevent alarms from being raised every time a signal condition occurs briefly, and to prevent the alarm from being deactivated every time the signal condition temporarily flickers off.

The alarm integration algorithm

The alarm integration algorithm uses two values: the alarm integration time and the decay rate. (On the DataSMART the alarm integration time is set to 2.5 seconds and the decay rate is 1/5.)

The algorithm maintains a count for each signal condition. Whenever a signal condition exists, time accrues to the count for that signal condition. For instance, if the OOF signal condition exists for 1 second, 1 second is accrued to the OOF count. Time spent out of the signal condition is multiplied by 1/5 (the decay rate) and subtracted from the count, which has a minimum value of 0. When the count exceeds 2.5 (the alarm integration time), the transition to an alarm state occurs.

The alarm integration algorithm is defined in detail in AT&T 62411.

Transitioning out of the alarm state

When a signal condition that has produced an alarm goes away, the alarm persists until the condition has been absent for a period of time referred to as the alarm deactivation time. The alarm deactivation time is user-configurable and by default is 15 seconds. (See "Setting the alarm deactivation time" on page 67 for more information.)

Alarm reporting

The DataSMART produces an alarm message each time a line transitions to a new alarm state. The "CLR" message is not sent until all alarms on a particular interface clear. All alarm messages are output to the device connected to the control port and are logged in the Alarm History report. To see the Alarm History report, type **AHR** at the command line.

You can examine the current status and track the changing conditions on an interface using the System Status report (type **S** at the command line). This report shows the current alarm state of the DataSMART as well as the signal condition of the input and output signal at all interfaces. The status report is updated once a second upon any changes to the alarm state or signal conditions. You can also track system status from the LCD display on the front panel of the DataSMART. See "Examining system status" on page 135 for more information.

A received T1 signal is classified as being in one and only one alarm state at a time. Alarm states have a priority. If the signal satisfies more than one of the requirements for an alarm state, the higher priority alarm applies. Because of this, and because of the delay of deactivation of an alarm, the System Status report could contain an entry in which an interface is in an alarm state that does not match the signal condition.

For example, suppose the alarm deactivation time period is set to 15 seconds, and suppose the signal condition for the NI received signal is AIS. After the alarm integration requirements are met, the line is declared to be in the AIS alarm state. Now suppose that the signal condition changes from AIS to OOF. At this point the DataSMART will add a new entry to the status report to show the change in the signal condition. However, in that same entry, the alarm condition will be shown as AIS because the alarm deactivation time period has not passed.

Now assume the OOF condition persists for 2.5 seconds, and thus has satisfied the conditions for alarm integration. Because the OOF has a lower priority, and because of the 15-second deactivation period for alarms, the alarm state will still be AIS. However, once the 15 seconds have passed, the alarm state will transition from AIS to OOF, and the DataSMART will add a new entry to the status report.

Signal conditions

The table below lists the signal conditions for the DataSMART in priority order, highest priority first. A received T1 signal can be in one and only one of the signal conditions at a time.

Condition	Definition
LOS	Loss of Signal. No pulses are being received. The LOS signal condition starts upon receipt of 192 consecutive spaces or zeros. The LOS signal condition clears when the signal contains 32 consecutive bits with at least 4 ones and no more than 15 consecutive zeros.
AIS	Alarm Indication Signal. A signal with a 99.9% ones density for a minimum of 3 milliseconds and no framing detected is being received. The AIS condition is detected in the presence of a 1×10^{-3} bit error rate. An AIS condition is declared when both out-of-frame and all 1s conditions are present at the interface. The AIS condition clears when either the OOF, all 1s, or both conditions clear.
OOF	Out of Frame. The received signal does not contain a T1 framing pattern. The OOF signal condition is declared when two out of four frame bits are in error (SF and Ericsson framing) or when two out of six frame bits are in error (ESF framing). The OOF signal condition clears when a reframe occurs.
EER	Excessive Error Rate. A framed T1 signal with an event error rate exceeding the user-supplied threshold is being received. This condition clears when the next time interval's error count is less than the threshold.
YELLOW	The received signal contains the yellow alarm pattern in bit two of each DS0 (SF framing) or a yellow alarm code word in the ESF Data Link (ESF framing). The condition clears when the yellow alarm pattern is no longer detected in the received signal.
Good Signal	A framed T1 signal with none of the above listed signal conditions.

Alarms

For each of the signal conditions described in the previous table there is an alarm state. The table below lists the T1 alarms for the DataSMART in priority order, highest priority first. Note that, as shown in the table, not all alarms use the alarm integration algorithm described on page 214.

Alarm	Definition
LOS	The LOS alarm starts upon a total of 2.5 seconds of alarm integration time spent in the LOS signal condition (the alarm integration time has a decay rate of 1/5 in case of an intermittent LOS signal condition). The LOS alarm clears after a continuous time period of *n* seconds with no LOS signal condition, where *n* is the alarm deactivation time period set by the user via the DACT command.
AIS	The AIS alarm starts upon a total of 2.5 seconds of alarm integration time spent in the AIS signal condition (the alarm integration time has a decay rate of 1/5 in case of an intermittent AIS signal condition). The AIS alarm clears after a continuous time period of *n* seconds with no AIS signal condition, where *n* is the alarm deactivation time period set by the user via the DACT command.
OOF	The OOF alarm starts upon a total of 2.5 seconds of alarm integration time spent in the OOF signal condition (the alarm integration time has a decay rate of 1/5 in case of an intermittent OOF signal condition). The OOF alarm clears after a continuous time period of *n* seconds with no OOF signal condition, where *n* is the alarm deactivation time period set by the user via the DACT command.
Yellow Alarm	The yellow signal alarm is declared after receiving the yellow signal for 1 second. Once declared, the alarm stays active for a minimum of one second. It is cleared upon detection of an input signal without the yellow alarm pattern present.
EER	The EER alarm starts immediately upon entering the EER signal condition. The EER alarm clears after a continuous time period of *n* seconds with no EER signal condition, where *n* is the alarm deactivation time period set by the user via the DACT command.
Clear	None of the above listed alarms is active.

Specifications

Table 10—Environmental specifications

	Parameter	Specification
Temperature	Storage	-20°C to 66°C (5% to 65% RH)
	Operating	0°C to 50°C (5% to 90% RH, non-condensing)
Powering	AC input range	85 to 130 VAC, 47 to 63 Hz
	Power interruptions	Loss of power does not damage the unit. Loss of power for less than five years does not change the configuration settings which may have been set by the user. Loss of power for less than two hours (nominal) does not affect the real-time clock setting.

Table 11—Physical specifications

	Parameter	Specification
	Size with feet	1.7 inches by 7.75 inches by 11.5 inches
	Size without feet	1.65 inches by 7.75 inches by 11.5 inches
	Weight	Approximately 2.5 pounds

Table 12—Electrical interface specifications - network interface

	Parameter	Specification
Common	Line rate	Internal or external clock; 1.544 Mb/s $\pm$ 50 bps When timing is derived from input signal: 1.544 Mb/s $\pm$ 200 bps. Output line rate follows input line rate.
	Line Code	AMI or B8ZS (selectable).
	Line Impedance	100 ohms $\pm$ 10 ohms at 772 kHz 100 ohms $\pm$ 20% over the frequency band 100 kHz to 1Mhz
	Lightning Protection	Lightning surges defined per FCC Part 68 shall not damage the unit.
	Framing Format	SF or ESF per ANSI T1.403-1989, and TR-54016-1989; Ericsson Framing (defined as valid F_T bits only)
Input Only	Input Level	DSX-1 to -27.5 dB.
	Input Jitter Tolerance	Per TR 62411-1990 (p. 4.7.1)

Table 12—Electrical interface specifications - network interface (continued)

	Parameter	Specification
Output Only	Output Level	Per ANSI T1.403-1989 3.0 Volt peak ± 10% into 100 ohms at output connector
	Output Signal	Tolerant to impedance mismatches
	Line Build Out	0, 7.5, 15.0 selectable
	Output Jitter	TR 62411-1990 (p 4.7.2)
	Jitter Transfer	DSU: TR 62411-1990 (p 4.7.3)
	Pulse Density	(When enabled) shall be > 12.5%

Table 13—Electrical interface specifications - terminal interface

	Parameter	Specification
Common	Line rate	Internal; 1.544 Mb/s ± 50 bps When timing is derived from input signal: 1.544 Mb/s ± 200 bps. Output line rate follows input line rate.
	Line Code	AMI or B8ZS (selectable).
	Line Impedance	100 ohms ± 10 ohms at 772 kHz 100 ohms ± 20% over the frequency band 100 kHz to 1Mhz
	Framing Format	SF or ESF per ANSI T1.403-1989, and TR-54016-1989; Ericsson Framing (defined as valid F_T bits only) Idle ESF Data Link is set to 1s.
Input Only	Input Level	DSX-1 to -10.0 dB.
	Input Jitter Tolerance	Per TR 62411-1990 (p. 4.7.1)
	Input Jitter Transfer	Per TR 62411-1990 (p. 4.7.2)
Output Only	Output Level	DSX-1 at connector (no equalization enabled)
	Equalization	Up to 655 feet selectable, 5 steps

Table 14—Serial control port specification

	Parameter	Specification
	Baud Rate	2400, 9600, 19200, 38400
	Electrical Interface	EIA-574
Connector	DCE	DB9S
	DTE	DB9P

Table 15—Control port pin assignments

CCITT	Pin	Signal name	DTE	DCE
125	9	Ring Indicator (RI)	INPUT	OUTPUT
109	1	Rec Sig Det (DCD)	INPUT	OUTPUT
108.2	4	DTE Ready (DTR)	OUTPUT	INPUT
102	5	Signal GND		
104	2	Received Data	INPUT	OUTPUT
103	3	Transmit Data	OUTPUT	INPUT
106	8	Clear To Send (CTS)	INPUT	OUTPUT
105	7	Request To Send (RTS)	OUTPUT	INPUT
107	6	Data Set Ready (DSR)	INPUT	OUTPUT

Table 16—Data port interface specification

Parameter	Specification
Bit Rates	56 kHz to 1536 kHz
Connector	34-pin MRAC34S connector
Electrical Interfaces	V.35 Compatible
Interface Type	DCE

The following table shows V.35 pin assignments for the data port socket. Pin identifiers (A, B, etc.) appear on the plug and socket.

Table 17—V.35 connector pin assignments for data port

Pin	Designator ITU/EIA	Circuit Name	Source
A		Shield	
B	102/AB	AB, Signal Ground	
C	(a) 105/CA	CA (A), RTS	DTE
D	(a) 106/CB	CB (A), CTS	DCE
E	(a) 107/CC	CC (A), DSR	DCE
F	(a) 109/CF	CF (A), Received Line Signal Detector (DCD)	DCE
H	(a) 108.2/CD	CD (A), DTR	DTE
K		Local Data Terminal Loopback	DTE
L		Local Data Terminal Loopback	DTE
P	(a) 103/BA	BA (A), Transmitted Data A	DTE
S	(b) 103/BA	BA (B), Transmitted Data B	DTE
R	(a) 104/BB	BB (A), Received Data A	DCE
T	(b) 104/BB	BB (B), Received Data B	DCE
U	(a) 113/DA	DA (A), External Clock	DTE
W	(b) 113/DA	DA (B), External Clock	DTE
V	(a) 115/DD	DD (A), Receiver Signal Element Timing	DCE
X	(b) 115/DD	DD (B), Receiver Signal Element Timing	DCE
Y	(a) 114/DB	DB (A), Transmit Signal Element Timing	DCE
AA	(b) 114/DB	DB (B), Transmit Signal Element Timing	DCE

Figure 18—DataSMART 600 series V.35 data port jack

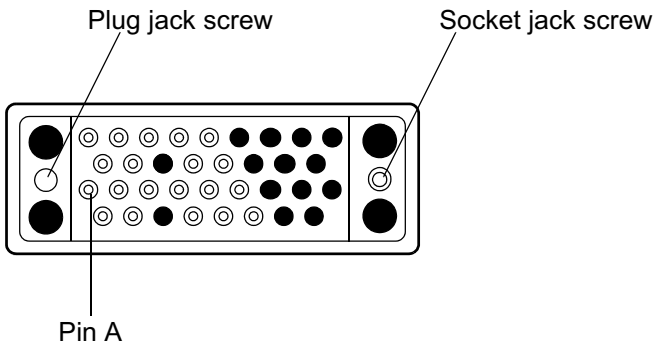


Table 18—Network interface pinout for the DA15 plug

Pin number	Circuit name
1	TxD data (R)
2	Frame ground
3	RxD data (R1)
4	Frame ground
9	TxD data (T)
11	RxD data (T1)
5, 6, 7, 8, 10, 12, 13, 14, 15	Not used

Table 19—Network interface pinout for the 8-pin RJ48C connector

Pin number	Circuit name
1	RxD data (T1)
2	RxD data (R1)
4	TxD data (T)
5	TxD data (R)
7,8	Optional shield
3, 6	No connection

Table 20—Terminal interface pinout for the DA15 socket

Pin number	Circuit name
1	TxD data (R1)
2	Frame ground
3	RxD data (R)
4	Frame ground
9	TxD data (T1)
11	RxD data (T)
5, 6, 7, 8, 10, 12, 13, 14, 15	Not used

Figure 19—Location of pin 1 on an RJ48C plug

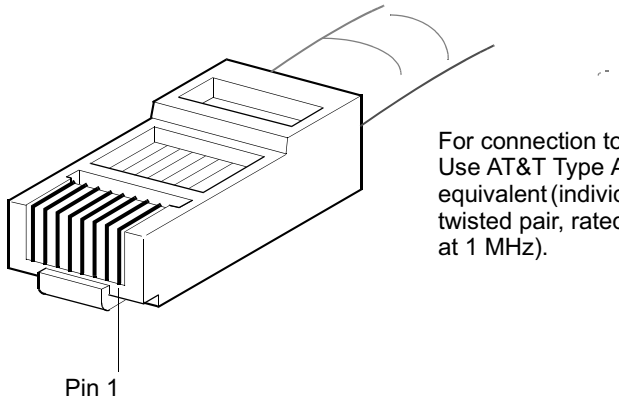


Figure 20—Data transmission interfaces

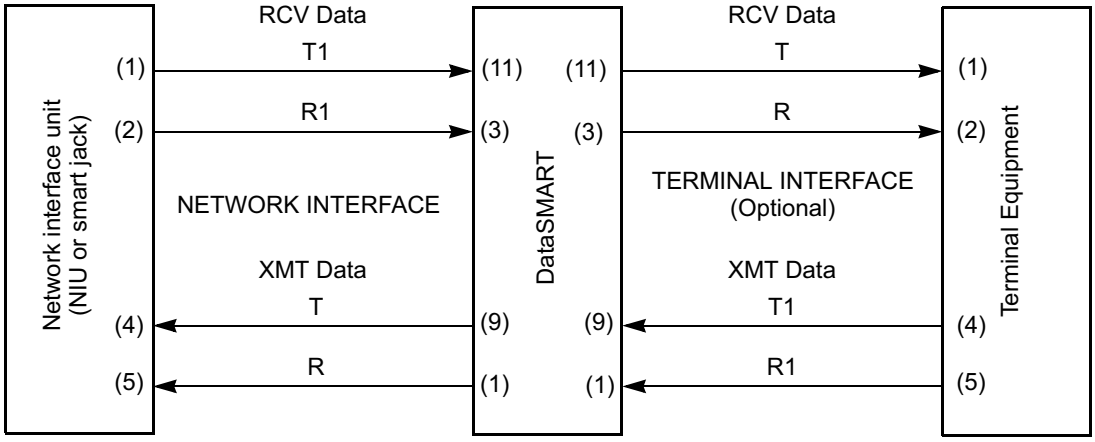


Table 21—Ethernet 10Base-T pinout

Pin Number	Signal
1	TD+
2	TD-
3	RD+
6	RD-
4	Unused
5	Unused
7	Unused
8	Unused

Table 22—Compatibility

Standard
AT&T TR54016 Issue 2, (TR62411/1990)
AT&T TR54019 Appendix A (Fractional T1)
EIA T1.403/1994
TIA-547

Table 23—Supported loopbacks

Loopback	Definition
LLB Line loopback	A minimum penetration loopback at the NI interface.
PLB Payload loopback	An interior loopback, looping the payload back to the NI.
DPLB Data Port loopback	Looping the bit stream assigned to the designated data port back towards the NI.
DTLB Data Terminal loopback	Looping the bit stream back to the data terminal equipment connected to the data port.
LOC Local loopback	An interior loopback, looping only the payload back to the Terminal Interface or data ports.
TILB Terminal Interface loopback	A minimum penetration loopback at the TI interface.

Glossary

2047 A test code pattern used for fractional T1 line testing.

3 in 24 A test code pattern used for testing a full T1 line.

511 A test code pattern used for fractional T1 line testing.

AIS Alarm Indication Signal. A signal condition and alarm indicating that the signal has been lost somewhere upstream. When a device experiences a loss of signal, it transmits an AIS signal to the next device downstream.

alarm An unsolicited message from a device that typically indicates a problem with a line.

all 0s A test code pattern used for testing a full T1 line.

all 1s A test code pattern used for testing a full T1 line.

auto-logout A feature that automatically logs out a user if there has been inactivity for a specified length of time.

BERT Bit Error Rate Test. A utility that tests a line's physical-layer (T1) performance and is used to isolate faulty lines. To troubleshoot a line, the first step is to send a test pattern (often utilizing a loopback to return the code to the device that initiated the test). BERT analyzes the signal to see if the line has caused errors in the pattern. By progressively testing segments of the circuit, the tester can discover which portion of the line is causing the problem.

BES Bursty Errored Second. Any second that is not a UAS that contains no LOS, AIS, or OOF conditions, and between 2 and 319 (inclusive) error events.

BPV Bipolar Violation. An unintentional disruption of the normal pattern of alternating high and low signals on a line. In a bipolar violation, two high signals occur without an intervening low signal, or vice versa. Some line coding methods include intentional bipolar events.

carrier A company, such as any of the "baby Bell" companies, that provide network communications services, either within a local area or between local areas.

CCS Common channel signaling.

channel A single communication path created, in the case of a T1 line, by multiplexing. A T1 line carries 24 channels, each with a bandwidth of 64 Kbps.

cold-start trap An SNMP trap that is sent when the unit has been power-cycled. *See also* trap.

command-line interface One method for accessing the management functions of the DataSMART unit, characterized by typing commands at a video display terminal. *See also* front-panel interface.

control port A port, either DTE or DCE, on the DataSMART unit to which you can connect a terminal, modem, or SLIP device, and that provides access to the DataSMART management functions. Control ports are also used to daisy-chain DataSMART units.

controlled slip A situation in which one frame's worth of data is either lost or replicated. Controlled slips are an indication of network timing problems. A controlled slip typically occurs when a DataSMART unit is not using the same clock as the unit that generated the received signal.

CPE Customer Premise Equipment. Equipment on the customer side of the point of demarcation, as opposed to equipment that is on a carrier side. *See also* point of demarcation.

CRC Cyclic Redundancy Check.

CSS Controlled Slip Second. Any second that contains one or more controlled slips (see also the definition for ES). CSSs are accumulated during unavailable seconds (UASs).

CSU *See* DSU/CSU.

CTS Clear To Send. Hardware flow-control on a control port or data port. A DataSMART unit can be set to monitor the data port for assertion of CTS. In this mode, if CTS is not asserted, a data port loss of signal alarm is generated.

daisy-chain A string of DataSMART units that have been interconnected so that they can all be managed from one terminal.

data port A port on a DSU to which some or all of the channels of a DS1 line can be routed.

datagram A packet of information used in a connectionless network service that is routed to its destination using an address included in the datagram's header.

DCE Data Communications Equipment. A definition in the RS232C standard that describes the functions of the signals and the physical characteristics of an interface for a communication device such as a modem.

DM Degraded Minute. A non-UAS and non-SES sixty-second period that contains 49 or more CRC4 errors or 49 or more bipolar violations.

dotted decimal notation A convention which represents an IP address or netmask (a 32-bit binary number) as a series of four decimal numbers between 0 and 255, separated by periods.

DS1 A standard that specifies an interface operating at 1.544 mbps (million bits per second)

and 24 discrete data channels that runs on a T1 line. In common usage, DS1 is synonymous with T1.

DSU/CSU Data Service Unit/Channel Service Unit. A DSU is a device that makes the link between a T1 line and a line that is carrying packetized data streams such as those produced by a router. A CSU is a device that makes the link between a T1 line and a line that is carrying raw data streams such as those produced by a PBX. A DSU/CSU combines the two functionalities.

DTE Data Terminal Equipment. A definition in the RS-232C standard that describes the functions of the signals and the physical characteristics of an interface for a terminal device such as a terminal.

DTR Data Terminal Ready. Hardware flow-control on a control port or data port. A DataSMART unit can be set to monitor the data port for assertion of DTR. In this mode, if DTR is not asserted, a data port loss of signal alarm is generated.

ECF External Clock Input Failure. An alarm generated by a DataSMART unit that is configured for external clocking and has lost the clocking signal.

EER Excessive Error Rate. An alarm which indicates that a threshold for the number of errored seconds or unavailable seconds has been exceeded.

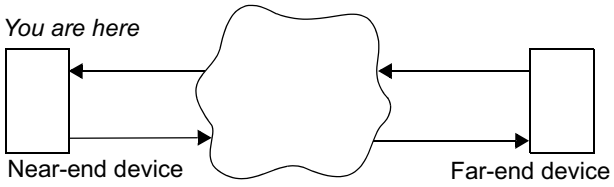
embedded SNMP agent An SNMP agent can come in two forms: embedded or proxy. An embedded SNMP agent is one that is integrated into the physical hardware and software of the unit. DataSMART has an internal, integrated SNMP agent. Advantages to this approach are time-accuracy of data and fast response time. *See also* proxy SNMP agent.

EQF Internal Equipment Failure. Something has happened to cause the internal hardware of the DataSMART unit to fail. The unit needs to be serviced.

ES Errored Second. A measurement of the quality of the signal on a T1 line defined as any second that is not an unavailable second and that contains one or more CRC6 errors.

ESF Extended Super Frame.

far-end In a relationship between two devices in a circuit, the far-end device is the one that is remote.



FDL Facility Data Link. A link embedded in the ESF framing bits that is used for such things as accessing performance data on remote units, remote log in, and carrier access to the DataSMART unit.

fractional T1 A service in which the carrier provides only a subset of the full 24 channels of a T1 line.

frame relay A packet-oriented communication protocol.

frame slip *See* controlled slip.

host A device on an IP network.

ICMP Internet Control Message Protocol. ICMP is a protocol in the TCP/IP suite of protocols that is used to determine if a host is alive and responding. An ICMP query is referred to as a Ping. The response is either an "I can hear you" message, or simply no response. DataSMART will respond to Ping requests, but does not generate them.

IP Internet Protocol. A suite of protocols for packetizing data for shipment across LANs and WANs. Protocols exist above the IP protocol for transmitting and receiving IP packets. DataSMART uses the IP protocol to provide SNMP and Telnet access.

IP address A unique 32-bit integer used to identify a device in an IP network. You will most commonly see IP addresses written in "dot" notation; for instance, 192.228.32.14. *See also* IP netmask.

IP netmask A pattern of 32 bits that is combined with an IP address to determine which bits of an IP address denote the network number and which denote the host number. Netmasks are useful for subdividing IP networks. IP netmasks are written in "dot" notation; for instance, 255.255.255.0. *See also* IP address.

link-down trap An SNMP trap that signifies that the T1 line has transitioned from a normal state to an error state, or that a data port has been disconnected.

link-up trap An SNMP trap that signifies that the T1 line or a data port has transitioned from an error condition to a normal state.

LOFC Loss of Frame Count. An LOFC is the accumulation of the number of times a Loss of Frame is declared. On detection of an LOS or OOF, a rise-slope type integration process starts that declares a Loss of Frame after 2.5 (±0.5) seconds of continuous LOS or OOF. If the LOS or OOF is intermittent, the integration process decays at a slope of 1/5 the rise slope during the period when the signal is normal. Thus, if the ratio of an LOS or OOF to a normal signal is greater than 1/5, a Loss of Frame is declared. If during a one-second interval, but no more than 15 contiguous one-second intervals, no LOS or OOF conditions occur, the Loss of Frame condition is cleared.

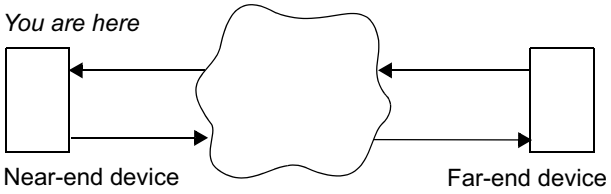
loopback A troubleshooting technique that returns a transmitted signal to its source so that the signal can be analyzed for errors. Typically, a loopback is set at various points in a line until the section of the line that is causing the problem is discovered.

LOS Loss of Signal. A signal condition and alarm in which the received signal at the network interface is lost.

MIB Management Information Base. The information that SNMP can access, structured as a hierarchy. In common usage of the term, MIB is in reference to a sub-branch of the entire MIB. DataSMART uses MIB II, the DS1 MIB and a product-specific enterprise MIB.

modem Modulator/demodulator. A device for converting a digital signal to analog (and vice versa) so that it can be transmitted over phone lines.

near-end In a relationship between two devices in a circuit, the near-end device is the one that is local.



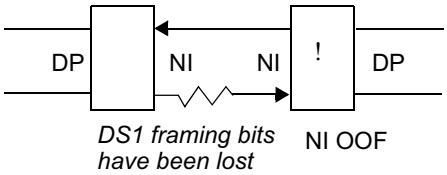
NI Network interface. The interface between the DataSMART unit and the T1 line supplied by the carrier.

NMS Network Management System. A tool for configuring network devices and monitoring network performance, typically an SNMP-based tool.

OID Object Identifier. The address of a MIB variable.

ones (1s) density A characteristic of a T1 line that refers to the rate at which 1s occur on the line. Because devices such as DataSMART cannot track a bit pattern using 0s, it loses synchronization if the 1s density is not high enough.

OOF Out of frame. A signal condition and alarm in which some or all of the DS1 framing bits are lost.



ping A protocol that is part of the TCP/IP suite, used to test the connectivity of the network. Ping sends a signal to a host or gateway, then listens for an echo response. *See* ICMP.

point of demarcation The dividing line between a carrier and the customer premise that is governed by strict standards that define the characteristics of the equipment on each side of the demarcation. Equipment on one side of the point of demarcation is the responsibility of the customer. Equipment on the other side of the point of demarcation is the responsibility of the carrier.

PPP Point-to-Point Protocol. A protocol that allows the Internet Protocol (IP) to run on low-speed serial lines. Unlike SLIP, it includes error correction. *See also* SLIP.

PRM Performance Report Message. Messages that are received once per second from a far-end device that report information about the condition of the far-end device.

proxy SNMP agent SNMP agents come in two forms: embedded and proxy. A proxy agent is physically outside of the device being managed. The proxy is a translator between the device's native command language and SNMP. Advantages of proxy agents are management of legacy equipment which cannot support embedded SNMP agents, and management of large numbers of devices where network connections may be limited. *See also* embedded SNMP agent.

QRS Quasi-Random Signal. A test code pattern used for testing a full T1 line.

real-time clock A clock that maintains the time of day in distinction to a clock that is used to time the electrical pulses on a circuit.

router A device that connects various links in a network matrix, directing packets along the most economical or efficient routes to the packet's destination; a packet switch.

RxD Received Data. The control ports and data ports on DataSMART units have an RxD line. This line is defined from the DTE perspective, so RxD for a DCE port is actually TxD. Each data port has a pair of RxD and TxD LEDs on the front panel. See *also* TxD.

SES Severely Errored Second. Any second that is not a UAS that contains an LOS condition, an AIS condition, an OOF condition, or 320 or more error events.

SF Super Frame.

signal condition Characteristics of the electronic pulses on a line, categorized into groups of various error types. When errored signal conditions persist they cause DataSMART to raise an alarm.

SLIP Serial Line Internet Protocol. A protocol that allows the Internet Protocol (IP) to run on low-speed serial lines.

SMDS Switched Multi-Megabit Digital Service. A public, high-speed, connectionless, packet-switched data transfer service that provides LAN-like performance and features over an entire metropolitan area.

SNMP Simple Network Management Protocol. The accepted industry-standard network management protocol that uses a system of agents and managers. Each agent is responsible for interacting with a certain MIB. The manager can ask the agent for data, or it can ask the agent to set the value of some data.

super-user A login ID that allows unlimited access to the full range of a device's functionality, especially including the ability to reconfigure the device and set passwords.

T1 A specification for a transmission line. The specification details the input and output characteristics and the bandwidth. T1 lines run at 1.544 Mbps and provide for 24 data channels. In common usage, the term "T1" is used interchangeably with "DS1."

TCP Transport Control Protocol. TCP is one of the two transport protocols in the TCP/IP protocol suite. TCP is a complex, connection-based protocol that guarantees reliable delivery of packets. Telnet uses TCP.

TCP/IP A suite of protocols that includes IP, UDP, TCP, SNMP, Telnet, ICMP, and PING. TCP/IP is the networking protocol of choice of the Internet and many private networks as well. Kentrox SNMP and Telnet products operate in TCP/IP networks.

Telnet Telnet is a TCP/IP protocol that defines a client/server mechanism for emulating directly-connected terminal connections. DataSMART implements a Telnet Server, allowing other devices to establish connections with it. DataSMART does not implement a Telnet Client (which would allow DataSMART to connect to other devices).

terminal server In the simplest terms, a terminal server is an IP network port and a collection of serial ports. Most terminal servers allow the serial ports to be configured for SLIP. If a DataSMART unit is using SLIP for its IP network connection, a terminal server could be used to make the connection from serial to Ethernet.

trap A trap is an unsolicited alert generated by SNMP. There are five standard trap types: link up, link down, warm start, cold start, and enterprise-specific.

TxD Transmit Data. The control ports and data ports on DataSMART have a TxD line. This line is defined from the DTE perspective, so TxD for a DCE port is actually RxD. Each data port has a pair of RxD and TxD LEDs on the front panel. *See also* RxD.

UAS Unavailable Second. A measurement of the signal quality of a T1 line. Unavailable seconds start accruing when ten consecutive severely errored seconds occur.

UDP User Datagram Protocol. One of the two transport protocols in the TCP/IP protocol suite. UDP is a send and forget protocol, which means there is no guarantee that the datagram will reach its destination.

V.35 An interface specification for serial communications that can handle data at higher speed than the RS232 interface.

VDT Video Display Terminal.

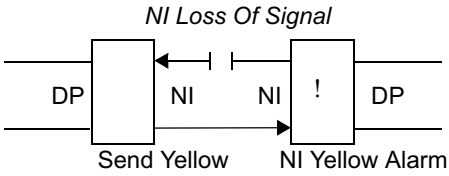
virtual circuit A transmission stream that is established between two points before they can exchange data packets in a frame-based service.

warm-start trap One of the five SNMP trap types. For Kentrox equipment, warm start traps indicate that SNMP alarm messages or agents have been enabled.

Xon/Xoff This is software flow control for the control ports. When a DataSMART unit has too much data coming in, it will transmit an Xoff (stop transmitting) character. If the device on the other end understands flow control, it will stop transmitting until it receives an Xon (resume transmitting) character. If the DataSMART unit receives an Xoff, it stops

transmitting data until it receives an Xon. Xon/Xoff flow control is not available when SLIP is enabled.

yellow alarm An alarm that occurs on a device when the signal from the device is not received at the far end.



Index

Symbols

Numerics

A

B

C

D

E

F

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Y

Z